

Draft **EN 301 060-1** V1.1.1 (1997-08)

European Standard (Telecommunications series)

**Integrated Services Digital Network (ISDN);
Digital Subscriber Signalling System No. one (DSS1) protocol;
Basic call applications enhancement at the "b" service entry
point for Virtual Private Network (VPN) applications;
Part 1: Protocol specification**



European Telecommunications Standards Institute

Reference

DEN/SPS-05109-1 (9tc90ico.PDF)

Keywords

Basic, DSS1, ISDN, VPN

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>

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

Contents

Intellectual Property Rights.....	5
Foreword	5
1 Scope.....	6
2 References.....	6
2.1 Normative references.....	7
2.2 Informative references	7
3 Definitions.....	7
4 Abbreviations	9
5 Description.....	9
5.1 VPN services in the context of CN	9
5.2 Networking aspects - requirements	11
5.2.1 Emulation of transit PINX functionality and gateway PINX functionality in the public network.....	11
5.2.1.1 Support of multiple CNs.....	11
5.2.2 Emulation of originating and/or terminating PINX functionality in the public network	12
5.2.2.1 Connection requirements	12
6 Emulation of PINX functionality.....	12
7 Coding requirements	13
7.1 Additional messages and content.....	13
7.1.1 SETUP message.....	13
7.1.2 CONNECT message	13
7.2 Additional information elements coding.....	13
7.2.1 Called party number	13
7.2.2 Calling party number.....	15
7.2.3 Connected number.....	16
7.2.4 Connected subaddress	16
7.2.5 Progress indicator.....	16
7.2.6 Transit counter	17
7.2.7 VPN indicator	17
8 Basic call states	18
9 Circuit-switched call control procedures	18
9.1 Distinction between public network and VPN context	18
9.2 Procedures applicable for signalling in a public network context.....	19
9.3 Procedures applicable for signalling in a VPN context.....	19
9.3.1 Establishment of calls from a physical PINX.....	19
9.3.1.1 Call request.....	19
9.3.1.2 Notification of interworking at the interface between a physical PINX and the public network equipment	19
9.3.1.3 In-band information provided to the physical PINX at the outgoing side.....	20
9.3.1.4 Call confirmation.....	20
9.3.2 Establishment of calls towards a physical PINX	21
9.3.2.1 Incoming call	21
9.3.2.2 Notification of interworking at the interface between a physical PINX and the public network equipment	21
9.3.2.3 In-band information provided by the physical PINX at the incoming side.....	22
9.3.2.4 Call confirmation	22
10 System parameters	22
Annex A (informative): Networking aspects - CN models	23
A.1 Representation of a CN in terms of functional groupings	23
A.1.1 Connections between PINXs.....	23

A.1.2	Structured overview of the functional groupings which may be involved in a call	24
A.1.3	Transit networking service provided by the public network.....	25
A.1.4	Transit and terminating functions provided by the public network	25
Annex B (informative):	Relationship between outgoing side and incoming side.....	27
History		28

Intellectual Property Rights

ETSI has not been informed of the existence of any Intellectual Property Right (IPR) which could be, or could become essential to the present document. However, pursuant to the ETSI Interim IPR Policy, no investigation, including IPR searches, has been carried out. No guarantee can be given as to the existence of any IPRs which are, or may be, or may become, essential to the present document.

Foreword

This draft European Standard (Telecommunications series) has been produced by ETSI Technical Committee Signalling Protocols and Switching (SPS), and is now submitted for the Public Enquiry phase of the ETSI standards Two-step Approval Procedure (TAP).

The present document defines the Digital Subscriber Signalling System No. one (DSS1) extensions to the basic call to support the Private Signalling System No. one (PSS1) information flow (see ISO/IEC 11572 [7]) in Virtual Private Network (VPN) applications. The relevant requirements and other information that affect DSS1 are defined in the present document.

The requirements for basic call in Private Integrated Services Networks (PISNs) are given in ETS 300 171 [10].

The present document is part 1 of a multi-part European Standard (Telecommunications series) covering the Integrated Services Digital Network (ISDN); Digital Subscriber Signalling System No. one (DSS1) protocol; Basic call applications enhancement at the "b" service entry point for Virtual Private Network (VPN) applications, as identified below:

- Part 1: "Protocol specification";**
- Part 2: PICS proforma specification;
- Part 3: Test Suite Structure and Test Purposes (TSS&TP), user;
- Part 4: Abstract Test Suite (ATS), user;
- Part 5: Test Suite Structure and Test Purposes (TSS&TP), network;
- Part 6: Abstract Test Suite (ATS), network.

Proposed national transposition dates	
Date of latest announcement of this EN (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	6 months after doa

1 Scope

The present document covers the application of a public Integrated Services Digital Network (ISDN) providing Virtual Private Network (VPN) services to Private Integrated Network eXchanges (PINX).

The present document contains only additional requirements to those in the main body of ETS 300 403-1 [2].

The present document specifies the additional basic call signalling requirements (extensions to the Digital Subscriber Signalling System No. one (DSS1) protocol) for the support of private network inter connection for VPN applications within the pan-European Integrated Services Digital Network (ISDN).

The present document specifies additional protocol elements and call control procedures for the handling of calls between users in a Corporate Network at the "b" service entry point. The functionality provided by the public network equipment may be:

- the emulation of an Originating PINX;
- the emulation of a Terminating PINX;
- the emulation of a Transit PINX;
- the emulation of a Relay Node;
- the emulation of an Incoming Gateway PINX;
- the emulation of an Outgoing Gateway PINX;
- the emulation of a combination of two or more of the above.

The support of these capabilities is a network option.

The present document does not cover the requirements for support of the "a" service entry point.

The specification included in the present document does not imply any specific implementation technology or platform.

NOTE : Calls/connections relating to the VPN "b" service entry point are distinguished from calls that are accessing the public network at the T reference point. Calls relating to the T reference point are supported in accordance with the requirements of ETS 300 403-1 [2]. Calls relating to the "b" service entry point are supported in accordance with the requirements of the present document. The requirements have been defined such that both contexts can coexist on the same access, and this is expected to be a typical implementation. There is no requirement that when the provisions of the present document are implemented, calls at the T reference point also need to be implemented on the same access. Where both contexts are implemented, the access resources are common to both contexts.

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 I.411 (1993): "ISDN user-network interfaces - reference configurations".
- [2] ETS 300 403-1 (1995): "Integrated Services Digital Network (ISDN); Digital Subscriber Signalling System No. one (DSS1) protocol; Signalling network layer for circuit-mode basic call control; Part 1: Protocol specification".
- [3] ETS 300 097-1: "Integrated Services Digital Network (ISDN); Connected Line Identification Presentation (COLP) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".
- [4] ITU-T Recommendation I.210 (1993): "Principles of telecommunication services supported by an ISDN and the means to describe them".
- [5] ITU-T Recommendation I.112 (1993): "Vocabulary of terms for ISDNs".
- [6] ISO/IEC 11571: "Information technology - Telecommunications and information exchange between systems - Numbering and sub-addressing in private integrated services networks".
- [7] ISO/IEC 11572: "Information technology - Telecommunications and information exchange between systems - Private Integrated Services Network - Circuit mode bearer services - Inter-exchange signalling procedures and protocol".
- [8] ISO/IEC 11579: "Information technology - Telecommunications and information exchange between systems - Private Integrated Services Network - Reference configuration for PINXs".
- [9] ISO/IEC 15056: "Information technology - Telecommunications and information exchange between systems - Private Integrated Services Network - Inter-exchange signalling protocol - Transit counter additional network feature".
- [10] ETS 300 171 (1992): "Private Telecommunications Network (PTN); Specification, functional models and information flows; Control aspects of circuit mode basic services; ECMA-BCSD".

2.2 Informative references

- [11] ITU-T Recommendation I.330: "ISDN numbering and addressing principles".

3 Definitions

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

Corporate telecommunication Network (CN): Consists of sets of equipment (Customer Premises Equipment (CPE) and/or Customer Premises Network (CPN)) which are located at geographically dispersed locations and are interconnected to provide networking services to a defined group of users.

NOTE 1: The ownership of the equipment is not relevant to this definition.

NOTE 2: In the present document, even equipment which is not geographically dispersed (e.g. a single PINX or Centrex-provided services to users at a single location) may form a CN.

End PINX functionality: Within the context of a call the functionality of a PINX required to provide attachment and servicing of terminals.

Gateway PINX functionality: Within the context of a call the functionality of a PINX required interconnect End PINXs or Transit PINXs with nodes of other public or private networks.

Incoming Gateway PINX functionality: Gateway PINX functionality providing support of calls incoming to the Corporate Network.

Integrated Services Digital Network (ISDN): See ITU-T Recommendation I.112 [5], definition 308.

Originating PINX functionality: End PINX functionality providing support of the calling user.

Outgoing Gateway PINX functionality: Gateway PINX functionality providing support of calls from the Corporate Network to other networks.

Private Integrated Network eXchange (PINX): A PISN nodal entity that provides automatic switching and call handling functions used for the provision of telecommunication services. The nodal entity can be implemented by one or more pieces of equipment located on the premises of the private network administrator or by equipment co-located with, or physically part of, a public network.

NOTE 3: If applicable, a PINX provides to users of the same and/or other private integrated services network exchanges:

- telecommunication services within its own area; and/or
- telecommunication services from the public ISDN; and/or
- telecommunication services from other public or private networks; and/or
- within the context of a PISN, telecommunication services from other PINXs.

relay node functionality: Within the context of a call the functionality that distinguishes calls between users in the Corporate Network, and relays such calls to designated PINX functionality emulated by public network equipment, or to a designated terminating "b" service entry point. This may be via other relay nodes. Relay Node functionality includes transparent handling of private networking information (e.g. transit counter).

service; telecommunications service: See ITU-T Recommendation I.112 [5], definition 201.

side; incoming side and outgoing side: The term side is used to describe either of the two PINXs at each end of an Inter PINX link, and in particular to describe the Private Signalling System No. one (PSS1) protocol entity within a PINX. In the context of a call, the Outgoing Side is the Side which routes the call over the Inter PINX link and the Incoming Side is the Side which receives the call (see annex B).

supplementary service: See ITU-T Recommendation I.210 [4], subclause 2.4.

Terminating PINX functionality: End PINX functionality providing support of the called user.

Transit PINX functionality: Within the context of a call the functionality of a PINX required to interconnect End PINXs and/or other Transit PINXs and/or Gateway PINXs.

Virtual Private Network (VPN): Is that part of a CN that provides corporate networking using shared switched network infrastructures. This is split into VPN architecture and VPN services.

The VPN architecture is that part of a CN that provides corporate networking between customer equipment where:

- the shared switch network infrastructure takes the place of the traditional analogue or digital leased lines and the function of the transit node, irrespective of the network type, whether it be the Public Switched Telephone Network (PSTN), ISDN, mobile communication network, or a separate network;
- the customer premises may be served in terms of end node functionality with any combination of PBX, Centrex, Local Area Network (LAN) router, or multiplexer;
- the CN user may also be served by terminal equipment connected to end node functionality residing on customer premises, or provided by public network equipment; and
- the VPN architecture in one network, or multiple networks, comprises a part of the total national or international CN.

VPN services offered by the switched network infrastructure provide:

- VPN end-user services to CN users;
- VPN networking services to support the interconnection of PINXs;
- service interworking functionality;
- inter-VPN services to provide co-operation between the VPN services of two networks; and

- VPN management services to enable service subscribers to control and manage their VPN resources and capabilities.

4 Abbreviations

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

ANF-TCSD	Additional Network Feature - Transit Counter
CLIP	Calling Line Identification Presentation supplementary service
CLIR	Calling Line Identification Restriction supplementary service
CN	Corporate telecommunication Network
COLP	COnnected Line identification Presentation supplementary service
COLR	COnnected Line identification Restriction supplementary service
CPE	Customer Premises Equipment
CPN	Customer Premises Network
DSS1	Digital Subscriber Signalling System No. one
IA5	International Alphabet No. five
ISDN	Integrated Services Digital Network
LAN	Local Area Network
PBX	Private Branch Exchange
PINX	Private Integrated Network eXchange
PISN	Private Integrated Services Network
PSS1	Private Signalling System No. one
PSTN	Public Switched Telephone Network
SUB	SUBaddressing supplementary service
TE	Terminal Equipment
VPN	Virtual Private Network

5 Description

The present document specifies the extensions required to the basic call control signalling protocol defined in ETS 300 403-1 [2] to support calls within a Corporate Network (CN) and to support calls which enter or exit the CN via Gateway PINX functionality performed by public network equipment. The protocol is applicable at the T reference points to which VPN services are provided. The support of these additional signalling capabilities is a network option. These Digital Subscriber Signalling System No. one (DSS1) extensions shall be made available to PINXs, on the basis of bilateral agreements at subscription time.

The additional basic call signalling capabilities identified in the present document are to provide information flows that are functionally identical to the information flows provided by the Private Signalling System No. 1 (PSS1) basic call control protocol (as defined by ISO/IEC 11572 [7]). In the context of the present document, the public network equipment (providing these VPN services) can be seen, from the private network perspective, as providing an interconnection between a PINX supporting the present document and another PINX supporting PSS1 information flows. This second PINX may be a physical PINX connected to the public network equipment or may be an emulation of an End PINX functionality provided by the public network equipment.

5.1 VPN services in the context of CN

The support of virtual private networking has been developed using the concept of "service entry points". This enables VPN services to be described without the need to identify impacts on particular protocols. Whilst the present document only relates to the "b" service entry point and to PINX type 2, the other service entry points are included for completeness. Items that are covered by the present document are specifically identified in the text.

Annex A provides more information on CN models.

In order to identify VPN services and the points where these services are offered (service entry points) the CN overview given in figure 1 has been produced. It reflects a CN overview in terms of services and service relations between:

- CPE/CPN;
- public networks;
- VPN service providers; and
- VPN service subscribers.

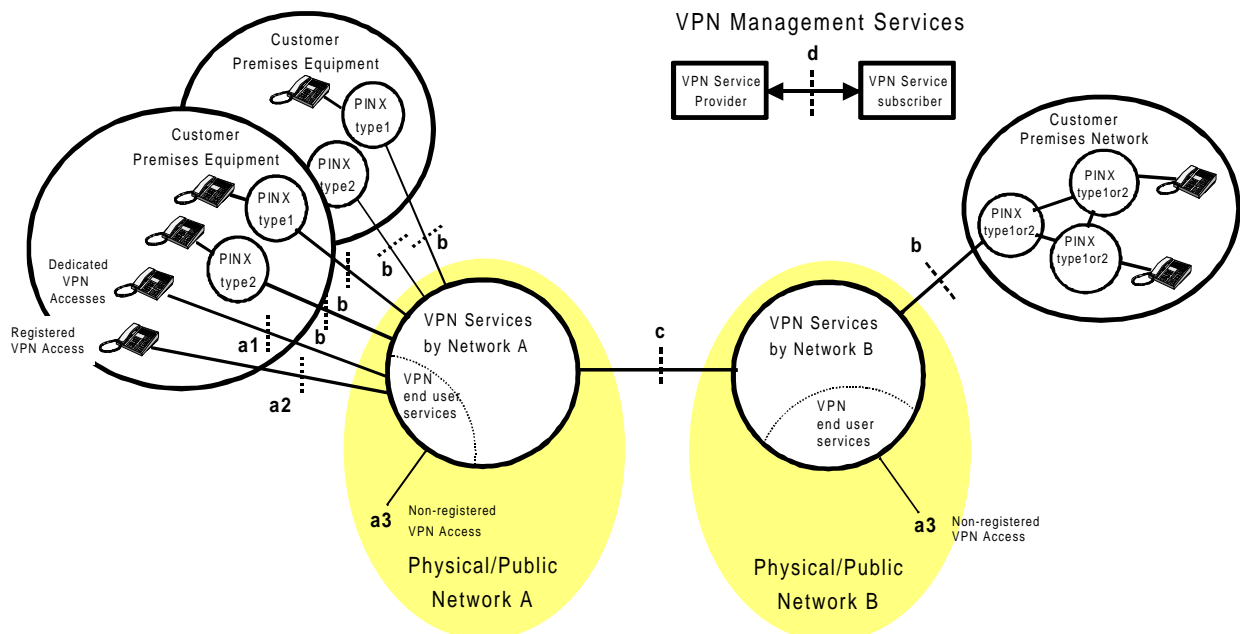
The following PINX types are defined:

PINX type 1: An implementation of a Private Integrated Network eXchange (PINX) outside the public network that supports services provided by the public ISDN and/or PSTN.

PINX type 2: An implementation of a Private Integrated Network eXchange (PINX) outside the public network that supports services based on PISN standards in addition to the services provided by the public ISDN and/or PSTN. The scope of the present document covers the support of PINX type 2.

Referring to figure 1, VPN services can be subdivided into four classes depending on the service entry point at which they are offered:

- VPN end-user services: services offered at the a1, a2 and a3 service entry points;
- VPN networking services: services offered at the b service entry point;
- Inter-VPN services: services offered at the c service entry point; and
- VPN management services: services offered at the d service entry point.



NOTE: a2 is a registered VPN access operating in the CN mode.

Figure 1: VPN services in context of a CN

The following types of service entry points are identified:

a1: The a1 service entry point for an access (within a specific CN) which is dedicated to the utilization of VPN services. This is referred to as "dedicated VPN access". At this service entry point, a pre-defined set of VPN end-user services is permanently available.

- a2: The a2 service entry point for a public network access which is registered as able to utilize VPN services within a predetermined CN. This is referred to as "registered VPN access". At this service entry point, the user can use either its pre-defined set of VPN end-user services, or the public network services.
- a3: The a3 service entry point for a public network access which is not registered for the utilization of VPN services. This is referred to as "non-registered VPN access". By means of an appropriate authentication procedure a pre-defined set of VPN end-user services becomes available to the CN user.
- b: The b service entry point for PINX type 2 and PINX type 1. At this service entry point VPN networking services are provided to PINX type 2 and PINX type 1 for the provision/support of services to its end-users. The scope of the present document covers the b service entry point and the support of PINX type 2.
- c: The c service entry point for the provision of inter-VPN services between different VPN service providers. At this service entry point co-operation between VPN service providers enables VPN services to span multiple public networks.
- d: The d service entry point between the VPN service provider and the VPN service subscriber for the offering of VPN management services. They allow the VPN service subscriber to manage resources and capabilities related to its CN.

5.2 Networking aspects - requirements

5.2.1 Emulation of transit PINX functionality and gateway PINX functionality in the public network

This subclause addresses some requirements for the emulation of transit PINX functionality, and for the emulation of gateway PINX functionality, in the public network. In general, the requirements are common to both and any requirements applying specifically to one type of functionality are indicated explicitly. Annex A contains a number of call examples to illustrate how the different functionality can interact.

NOTE: The requirements identified here need not be fulfilled in every switching element in the public network; these requirements need only be implemented at those switching elements in which CN functionality is needed.

The requirements for basic call functionality are identified in the following subclauses.

5.2.1.1 Support of multiple CNs

The public network can support the co-existence of multiple CNs in parallel, i.e. the resources of the public network are shared by multiple CNs. Each CN should be considered as a separate network.

The facilities of the virtual transit PINX or virtual gateway PINX are shared between the three CNs. Thus, the virtual transit PINX or virtual gateway PINX needs to be able to provide differentiation between the calls belonging to the different CNs.

The minimum requirement of the virtual transit PINX and the virtual gateway PINX is to be able to uniquely identify the CN to which a particular attached PINX belongs in order to ensure correct routing of a particular call. In addition, to ensure that calls do not terminate on incorrect CNs, a mechanism may be required at the point where the call leaves the public network.

In addition, a PINX may support multiple CNs. Thus the mechanism for identifying a CN needs to be conveyed between a PINX and the public network equipment.

The capability of supporting multiple CNs is fulfilled by the VPN indicator defined in subclause 7.2.7.

5.2.2 Emulation of originating and/or terminating PINX functionality in the public network

This subclause identifies the requirements for the emulation of originating and/or terminating PINX functionality in the public network. This is commonly known as Centrex. The requirements identified here are not required in every switching element in the public network, but only if and where required.

5.2.2.1 Connection requirements

Four types of network connections can be identified:

- connection to a PINX;
- connection through the CN (e.g. supported by the relay node functionality);
- access from a digital terminal (outside the scope of the present document); and
- access from an analogue terminal (outside the scope of the present document).

For connection to a PINX, the interface here is the same as that between two PINX.

6 Emulation of PINX functionality

The public network equipment may provide one or more of the following capabilities:

- the emulation of an Originating PINX;
- the emulation of a Terminating PINX;
- the emulation of a Transit PINX;
- the emulation of a Relay Node;
- the emulation of an Incoming Gateway PINX;
- the emulation of an Outgoing Gateway PINX.

For the emulation of Originating PINX functionality, the functions provided by the public network equipment shall meet the requirements of Originating PINX Call Control as defined in ISO/IEC 11572 [7] for the circuit-switched call control and the ISO supplementary services associated with the basic call (the Calling Line Identification Presentation supplementary service (CLIP), the Calling Line Identification Restriction supplementary service (CLIR), the COnnected Line identification Presentation supplementary service (COLP), the COnnected Line identification Restriction supplementary service (COLR), the SUBaddressing supplementary service (SUB)). In addition the Additional Network Feature - Transit Counter (ANF-TCSD) defined in ISO/IEC 11572 [7] may be supported by those extensions to the DSS1 protocol.

For the emulation of Terminating PINX functionality, the functions provided by the public network equipment shall meet the requirements of Terminating PINX Call Control as defined in ISO/IEC 11572 [7] for the circuit-switched call control and the ISO supplementary services associated to the basic call (CLIP, CLIR, COLP, COLR, SUB). In addition the transit counter additional network feature defined in ISO/IEC 11572 [7] may be supported by those extensions to the DSS1 protocol.

For the emulation of Transit PINX functionality, the functions provided by the public network equipment shall meet the requirements of Transit PINX Call Control as defined in ISO/IEC 11572 [7] for the circuit-switched call control and the ISO supplementary services associated to the basic call (CLIP, CLIR, COLP, COLR, SUB). In addition the transit counter additional network feature defined in ISO/IEC 11572 [7] may be supported by those extensions to the DSS1 protocol.

For Relay functionality, the public network equipment shall provide, as a minimum, the following at a minimum:

- minimal routing capability;
- transparent handling of private networking information (e.g. transit counter).

For the emulation of Incoming Gateway PINX functionality, the functions provided by the public network equipment shall meet the requirements of Incoming Gateway PINX call control as defined in ISO/IEC 11572 [7] for the circuit-switched call control and the ISO supplementary services associated to the basic call (CLIP, CLIR, COLP, COLR, SUB). In addition the transit counter additional network feature defined in ISO/IEC 11572 [7] may be supported by those extensions to the DSS1 protocol.

For the emulation of Outgoing Gateway PINX functionality, the functions provided by the public network equipment shall meet the requirements of Outgoing Gateway PINX call control as defined in ISO/IEC 11572 [7] for the circuit-switched call control and the ISO supplementary services associated to the basic call (CLIP, CLIR, COLP, COLR, SUB). In addition the transit counter additional network feature defined in ISO/IEC 11572 [7] may be supported by those extensions to the DSS1 protocol.

7 Coding requirements

7.1 Additional messages and content

No additional messages are defined. However, the content of some messages has additional requirements.

7.1.1 SETUP message

The VPN indicator information element may be included in the SETUP message in both the user-network and the network-user directions.

Inclusion of this information element is mandatory to indicate a VPN context.

The Called party number information element is mandatory in both the user-network and the network-user directions.

The Transit counter information element may be included in the SETUP message, for use in both user-to-network and network-to-user directions.

7.1.2 CONNECT message

The Connected number information element and the Connected subaddress information element may be included in the CONNECT message for use in both the user-network and the network-user directions.

7.2 Additional information elements coding

7.2.1 Called party number

Subclause 4.5.8 of ETS 300 403-1 [2] shall apply with the exception that table 4.9 of ETS 300 403-1 [2] shall be replaced by the following table:

Table 1: Called party number*Numbering plan identification (octet 3)*

Bits				
4	3	2	1	
0	0	0	0	Unknown (note 1)
0	0	0	1	ISDN/telephony numbering plan (Recommendation E.164)
1	0	0	1	Private numbering plan (ISO/IEC 11571)

All other values are reserved.

NOTE 1: The numbering plan "unknown" is used when the user or network has no knowledge of the numbering plan. In this case the number digits fields is organized according to the network dialling plan, e.g. prefix or escape digits might be present.

Type of number (octet 3) when Numbering Plan identification is ISDN/telephony numbering plan (Recommendation E.164) (note 2).

Bits			
7	6	5	
0	0	0	Unknown (note 3)
0	0	1	International number (note 4)
0	1	0	National number (note 4)
1	0	0	Subscriber number (note 4)

All others values are reserved.

NOTE 2: For the definition of international, national and subscriber number, see ITU-T Recommendation I.330 [11].

NOTE 3: The type of number "unknown" is used when the user or the network has no knowledge of the type of number, e.g. international number, national number, etc. In this case the number digits field is organized according to the network dialling plan; e.g. prefix or escape digits might be present.

NOTE 4: Prefix or escape digits shall not be included.

Type of number (octet 5) when Numbering Plan identification is Unknown

Bits			
7	6	5	
0	0	0	Unknown (note 3)

All others values are reserved.

NOTE 5: The type of number "unknown" is used when the user or the network has no knowledge of the type of number, e.g. international number, national number, etc. In this case the number digits field shall be organized according to the network dialling plan; e.g. prefix or escape digits might be present.

Type of number (octet 3) when Numbering Plan identification is Private numbering plan (note 6).

Bits			
7	6	5	
0	0	0	Unknown
0	0	1	Level 2 Regional Number
0	1	0	Level 1 Regional Number
0	1	1	PISN specific number
1	0	0	Level 0 Regional Number

All others values are reserved.

NOTE 6: For the definition of Level 2 Regional Number, Level 1 Regional Number, Level 0 Regional Number and PISN specific number, see ISO/IEC 11571.

Number digits (octets 4, etc.)

This field shall be coded with IA5 characters, according to the formats specified in the appropriate numbering/dialling plan.

7.2.2 Calling party number

Subclause 4.5.10 of ETS 300 403-1 [2] shall apply with the exception that table 4.11 of ETS 300 403-1 [2] is replaced by the following table:

Table 2: Calling party number

<i>Numbering plan identification (octet 3)</i>				
Bits				
4	3	2	1	
0	0	0	0	Unknown (Note 1)
0	0	0	1	ISDN/telephony numbering plan (Recommendation E.164)
1	0	0	1	Private numbering plan (ISO/IEC 11571)
All other values are reserved.				
NOTE 1: The numbering plan "unknown" is used when the user or network has no knowledge of the numbering plan. In this case the number digits fields is organized according to the network dialling plan; e.g. prefix or escape digits might be present.				
<i>Type of number (octet 3) when Numbering Plan identification is ISDN/telephony numbering plan (Recommendation E.164) (note 2)</i>				
Bits				
7	6	5		
0	0	0	Unknown (note 3)	
0	0	1	International number (note 4)	
0	1	0	National number (note 4)	
1	0	0	Subscriber number (note 4)	
All others values are reserved.				
NOTE 2: For the definition of international, national and subscriber number, see Recommendation I.330 [11].				
NOTE 3: The type of number "unknown" shall be used when the user or the network has no knowledge of the type of number, e.g. international number, national number, etc. In this case the number digits field is organized according to the network dialling plan; e.g. prefix or escape digits might be present.				
NOTE 4: Prefix or escape digits shall not be included.				
<i>Type of number (octet 3) when Numbering Plan identification is Unknown</i>				
Bits				
7	6	5		
0	0	0	Unknown (note 5)	
All others values are reserved.				
NOTE 5: The type of number "unknown" is used when the user or the network has no knowledge of the type of number, e.g. international number, national number, etc. In this case the number digits field is organized according to the network dialling plan; e.g. prefix or escape digits might be present.				
<i>Type of number (octet 3) when Numbering Plan identification is Private numbering plan (note 6).</i>				
Bits				
7	6	5		
0	0	0	Unknown	
0	0	1	Level 2 Regional Number	
0	1	0	Level 1 Regional Number	
0	1	1	PISN specific number	
1	0	0	Level 0 Regional Number	
All others values are reserved.				
NOTE 6: For the definition of Level 2 Regional Number, Level 1 Regional Number, Level 0 Regional Number and PISN specific number, see ISO/IEC 11571.				

(continued)

Table 2 (concluded): Calling party number*Presentation indicator (octet 3a)*

Bits		Meaning
7	6	Presentation allowed
0	0	Presentation restricted
1	0	Number not available due to interworking
1	1	Reserved

Screening indicator (octet 3a)

Bits		Meaning
2	1	User-provided, not screened
0	0	User-provided, verified and passed
1	0	Reserved
1	1	Network provided

Number digits (octets 4, etc.)

This field shall be coded with IA5 characters, according to the formats specified in the appropriate numbering/dialling plan.

7.2.3 Connected number

The coding of the Connected number information element shall be as defined in ETS 300 097-1 [3] subclause 7.1 with the exception that the content of this information element shall be coded as defined in subclause 7.2.2.

7.2.4 Connected subaddress

The coding of the Connected subaddress information element shall be as defined in ETS 300 097-1 [3] subclause 7.2.

7.2.5 Progress indicator

The following additional progress description values shall be as defined in the ISO/IEC coding standard ISO/IEC 11572 [7]:

Bits

765 4321 N°

001 0000 16 Interworking with a public network

001 0001 17 Interworking with a network unable to supply a release signal

001 0010 18 Interworking with a network unable to supply a release signal before answer

001 0011 19 Interworking with a network unable to supply a release signal after answer

When received from a physical PINX, they shall be transferred transparently by the public network equipment.

7.2.6 Transit counter

The Transit counter information element may be included in the SETUP message to indicate the number of private network transit exchanges which intervene in the requested connection. The Transit counter information element shall have a maximum length of 3 octets.

The Transit counter information element shall be defined in codeset 4.

bit	8	7	6	5	4	3	2	1	Octet	
	0	0	1	1	0	0	0	1	1	
Transit counter information element identifier										
Length of Transit counter										2
1	0 0		Transit count							3
Ext.	reserved		(binary value)							

7.2.7 VPN indicator

The VPN indicator information element shall be included in the SETUP message to indicate that the call is in VPN context.

The VPN indicator information element may, optionally, include a Business Group Identifier Parameter to distinguish between private networks in the VPN environment. The VPN indicator information element shall have a maximum length of 15 octets.

The VPN indicator information element is defined in codeset 0.

bit	8	7	6	5	4	3	2	1	Octet	
	0	0	0	0	0	1	0	1	1	
VPN indicator information element identifier										
Length of VPN indicator										2
1	Spare				Business Group indicator					3
Ext.										
Business Group Identification										4* ...
										15*

Business Group indicator (octet 3)

Bits

3 2 1

0 0 0 no indication (note 1)

0 0 1 local (note 2)

0 1 0 global (note 3)

All others values are reserved.

NOTE 1: When the Business Group indicator "no indication" is used, the call belongs to the assigned default Business Group. The corresponding global Business Group Identification is used for the call.

NOTE 2: When the Business Group indicator "local" is used, the Business Group Identification in octets 4 following indicates one of the subscribed Business Group Identifications. This value only has significance at the interface. The corresponding global Business Group Identification is used for the call.

NOTE 3: When the Business Group indicator "global" is used, the Business Group Identification in octets 4 following contains a globally unique value.

Business Group Identification (octets 4 to 15)

When the Business Group indicator is set to "no indication", no Business Group Identification shall be included.

When the Business Group indicator is set to "local", the Business Group Identification shall contain a binary coded index to a subscribed Business Group Identification.

When the Business Group indicator is set to "global", the Business Group Identification shall contain the binary representation of the Business Group Identification. The Business Group Identification starts with the BCD (Binary Coded Digit) representation of the E.164 country code digits of the country where the Business Group was initially assigned.

8 Basic call states

The call states shall apply unchanged, as defined in subclauses 2.1 and 2.4 of ETS 300 403-1 [2].

9 Circuit-switched call control procedures

9.1 Distinction between public network and VPN context

If an entity sends a message that establishes a call reference in a VPN context, that entity shall include a VPN indicator information element in this message.

If an entity receives a message that establishes a call reference, and this message does not contain a VPN indicator information element, then the procedures for signalling in a public network context for all messages that use this call reference shall apply.

If an entity receives a message that establishes a call reference, and this message contains a VPN indicator information element, then the procedures for signalling in a VPN context for all messages that use this call reference shall apply.

9.2 Procedures applicable for signalling in a public network context

For a call which is not identified as a call in a VPN context (see subclause 9.1), clause 5 of ETS 300 403-1 [2] shall apply.

9.3 Procedures applicable for signalling in a VPN context

For a call which is identified as a call in a VPN context (see subclause 9.1), clause 5 of ETS 300 403-1 [2] shall apply with the additions described in subclauses 9.3.1 and 9.3.2 of the present document.

9.3.1 Establishment of calls from a physical PINX

9.3.1.1 Call request

The physical PINX shall include the VPN indicator information element in the SETUP message.

The physical PINX shall include the Called party number information element in the SETUP message.

If received from the physical PINX, the Calling party number information element and the Calling party subaddress information element shall be handled as follows:

- a Transit PINX shall transfer the information elements to the next entity with PINX functionality, without taking into account any supplementary service subscription information;
- a Relay Node shall transfer the information elements to the next entity with PINX functionality without taking into account any supplementary service subscription information;
- an Outgoing Gateway PINX may transfer the information elements to the other network depending on the capability of the signalling system and whether the calling party number has significance in the other network. Translation of a number into the numbering plan of the other network may be performed in order to yield a number which has significance in the other network. If the received Calling party number information element has the presentation indicator value "presentation restricted", presentation of the number to the other network is outside the scope of the present document, but will depend on such factors as the other network's commitment to honour the restriction;
- a Terminating PINX may transfer the information elements to the called user, depending on any restrictions.

The physical PINX may include the Transit counter information element in the SETUP message. Whilst the handling of this information element by public network equipment is outside the scope of the present document, it shall be transferred as follows:

- a Transit PINX shall transfer the information element to the next entity with PINX functionality;
- a Relay Node shall transfer the information element to the next entity with PINX functionality;
- an Outgoing Gateway PINX may transfer the information elements to the other network depending on the capability of the signalling system; and
- a Terminating PINX shall not transfer the information to the user.

9.3.1.2 Notification of interworking at the interface between a physical PINX and the public network equipment

When the network receives a specific private network Progress description value from the physical PINX at the incoming side, it shall transfer it to the physical PINX at the outgoing side, without acting upon it.

Outgoing Gateway PINX functionality shall provide Progress indicator information elements as specified below and this information shall be transferred to the physical PINX. A Progress indicator information element shall be transmitted in a PROGRESS message, an ALERTING message or a CONNECT message as soon as the information becomes available, subject to a SETUP ACKNOWLEDGE or CALL PROCEEDING message having already been sent. A PROGRESS message shall be used unless an ALERTING or CONNECT message is to be sent at the time. All appropriate interworking indications shall be transmitted by the Outgoing Gateway PINX.

If the call has entered a public ISDN and a Progress indicator information element containing one of the following progress descriptions has been received from the public ISDN, that information element shall be passed on:

- 1 "call is not end-to-end ISDN, further call progress information may be available in-band";
- 2 "destination address is non-ISDN";
- 4 "call has returned to the ISDN";
- 8 "in-band information or appropriate pattern now available".

If the call is to enter another network (public or private) which is not ISDN, a Progress indicator information element may be sent containing progress description value 1 "call is not end-to-end ISDN, further call progress information may be available in-band".

The physical PINX at the outgoing side may optionally include any of the specific private network Progress description values in the SETUP message, to enable indication to the physical PINX at the incoming side delivery of particular situations at the originating side. The public network equipment shall transfer it to the physical PINX at the incoming side.

Up to three Progress indicator information elements may be included in a SETUP, ALERTING, PROGRESS and CONNECT message.

9.3.1.3 In-band information provided to the physical PINX at the outgoing side

The public network equipment may generate progress indications and may receive progress indications, e.g. due to interworking or from a physical PINX at the incoming side.

Upon receipt of a Progress description value #1 or #8, the public network equipment shall switch through in the backward direction.

Any progress indications shall be conveyed towards the physical PINX at the outgoing side.

Upon receipt of the Progress description value #1 or #8, the physical PINX at the outgoing side shall switch through in the backward direction to the B-channel in order to enable transfer of in-band tones/information and stop time T310 if running.

9.3.1.4 Call confirmation

The public network equipment shall include the Connected number information element and the Connected subaddress information element in the CONNECT message as follows:

- if received from an entity with PINX functionality, a Transit PINX shall transfer the information elements to the Physical PINX, without taking into account any possible supplementary service subscription information;
- if received from an entity with PINX functionality, a Relay Node shall transfer the information elements to the Physical PINX, without taking into account any possible supplementary service subscription information;
- an Outgoing Gateway PINX may transfer the information elements from the other network depending on the capability of the signalling system and whether the connected party number has significance in the Corporate Network. Translation of a number into the numbering plan of the Corporate Network may be performed in order to yield a number which has significance in the Corporate Network. If the received Connected number information element has the presentation indicator value "presentation restricted", presentation of the number to the Corporate Network is outside the scope of the present document; and

- a Terminating PINX shall generate (or complete any partial information received from the connected user) the Connected number information element to the physical PINX, without taking into account any possible service subscription information. Furthermore, a Terminating PINX shall transfer the Connected subaddress information element if received from the connected user, without taking into account any possible service subscription information.

9.3.2 Establishment of calls towards a physical PINX

9.3.2.1 Incoming call

The public network equipment shall include the VPN indicator information element in the SETUP message.

Incoming Gateway PINX functionality and Originating PINX functionality shall generate the VPN indicator information element if the information is not already available.

The public network equipment shall include the Calling party number information element and the Calling party subaddress information element in the SETUP message as follows:

- if received from an entity with PINX functionality, a Transit PINX shall transfer the information elements to the Physical PINX, without taking into account any supplementary service subscription information;
- if received from an entity with PINX functionality, a Relay Node shall transfer the information elements to the Physical PINX, without taking into account any possible service subscription information;
- an Incoming Gateway PINX may transfer the information elements from the other network depending on the capability of the signalling system and whether the connected party number has significance in the Corporate Network. Translation of a number into the numbering plan of the Corporate Network may be performed in order to yield a number which has significance in the Corporate Network. If the received Calling party number information element has the presentation indicator value "presentation restricted", presentation of the number to the Corporate Network is outside the scope of the present document; and
- an Originating PINX shall generate (or complete any partial information received from the calling user) the Calling party number information element to the physical PINX, without taking into account any possible service subscription information. Furthermore, an Originating PINX shall transfer the Calling party subaddress information element if received from the calling user, without taking into account any possible service subscription information.

The public network equipment shall include the Transit counter information element in the SETUP message if received from the physical PINX at the outgoing side.

9.3.2.2 Notification of interworking at the interface between a physical PINX and the public network equipment

The physical PINX at the incoming side may, optionally, include any of the specific private network Progress description values in the ALERTING, PROGRESS or CONNECT message returned to the public network equipment, to enable notification of particular situations at the incoming side. The public network equipment shall transfer the information as follows:

- a Transit PINX shall transfer the information elements to the next entity with PINX functionality;
- a Relay Node shall transfer the information elements to the next entity with PINX functionality;
- an Incoming Gateway PINX may transfer the information elements to the other network depending on the capability of the signalling system and if relevant; and
- an Originating PINX shall convey the information to the calling user - dependent on the ability of the calling user's equipment to receive such information.

Incoming Gateway PINX functionality shall provide Progress indicator information elements in the SETUP message as specified below and this information shall be transferred to the physical PINX. If none of the specified conditions apply, no Progress indicator information element shall be included.

If the call has arrived from a public ISDN and a Progress indicator information element containing one of the following progress descriptions has been received from the public ISDN, that information element shall be passed on:

- 1 "call is not end-to-end ISDN, further call progress information may be available in-band";
- 3 "origination address is non-ISDN".

If the call has entered the Corporate Network from a network (public or private) which is not ISDN, a Progress indicator information element may be sent containing progress description value 1 "call is not end-to-end ISDN, further call progress information may be available in-band".

When the public network equipment receives a specific private network Progress description value from the physical PINX at the outgoing side, it shall transfer it to the physical PINX at the incoming side, without acting upon it.

Up to three Progress indicator information elements may be included in a SETUP, ALERTING, PROGRESS and CONNECT message.

9.3.2.3 In-band information provided by the physical PINX at the incoming side

During call establishment, after the first message received in response to the SETUP message, on receipt of a Progress indicator information element with a progress description value #1 or #8 in the PROGRESS or ALERTING message, the public network equipment shall switch through in the backward direction to the allocated B channel in order to enable in-band tones/information provision from the destination private network to the user of the originating network, stop timer T310 if running and, if progress description #1 or #8 was received in the PROGRESS message while T310 was running, re-start timer T310.

The public network equipment shall transfer the Progress indicator information element towards the next entity with PINX functionality.

9.3.2.4 Call confirmation

The physical PINX may include the Connected number and the Connected subaddress information elements in the CONNECT message.

The Connected number information element and the Connected subaddress information element, when received from the physical PINX in the CONNECT message, shall be transferred by the public network equipment as follows:

- a Transit PINX shall transfer the information elements towards the next entity with PINX functionality, without taking into account any supplementary service subscription information;
- a Relay Node shall transfer the information elements to the next entity with PINX functionality, without taking into account any possible service subscription information;
- an Incoming Gateway PINX may transfer the information elements to the other network depending on the capability of the signalling system and whether the connected number has significance to the other network. Translation of a number into the numbering plan of the other network may be performed in order to yield a number which has significance in the other network. If the CONNECT message contains a Connected subaddress information element, the information element shall be conveyed unchanged to the other network if that network is a public ISDN. Where the other network is non-ISDN, Connected subaddress information may be conveyed to the other network if the signalling system permits. If the received Connected number information element has the presentation indicator value "presentation restricted", presentation of the number to the other network is outside the scope of the present document but will depend on such factors as the other network's commitment to honour the restriction; and
- an Originating PINX shall transfer the information elements to the calling user, depending on any restrictions.

10 System parameters

T310: the value of this timer when started or restarted upon receipt of progress description value 1 or 8 has a standard default value of 2 minutes (however, it can have different values in a range from 1 to 7 minutes).

Annex A (informative): Networking aspects - CN models

This annex provides background information on Corporate telecommunication Network (CN) environments and shows various network models (consisting functional groupings, service entry points and reference points) for calls in a CN. The models are used as a basis for development of the requirements, which are presented in clause 5 of the present document.

This annex provides some useful and relevant background information extracted from the ETSI Technical Report ETR 172 although it covers a wider scope from a functional point of view.

NOTE 1: The models do not include other aspects such as management aspects.

NOTE 2: The models should not be confused with stage 2 service modelling (i.e. the functional groupings are not the same as functional entities).

A.1 Representation of a CN in terms of functional groupings

Calls within a CN, calls originated outside the CN and calls terminating outside a CN can be represented by means of grouping functionality into "originating PINX", "terminating PINX", "transit PINX", and "gateway PINX" functions.

In the figures and their explanations below references to "originating PINX" should be understood as meaning "the implementation of the originating PINX functional grouping". This does not necessarily mean implementation in one (or more) physical PINX(s) as the public network may also provide originating and terminating functionalities.

A.1.1 Connections between PINXs

Figure A.1 shows functional groupings marked "IVN" together with a number of instances of Q reference points and also C reference points.

The IVN provides functionality which enables communication between functional groupings which are physically separated for a call (e.g. originating PINX and transit PINX). In such cases, an interface at the C reference point will exist. A relay node provides the functionality of an IVN.

The IVN functional grouping may be provided for example by:

- semi-permanent connections;
- an ISDN;
- a broadband ISDN; or
- a data communications network.

The Q reference point resides within a PINX and where an interface at the C reference point exists, there will be a mapping function within the PINX which converts from the Q reference point to the C reference point.

In figure A.1, the IVN functional grouping is only shown between the originating PINX functionality and the transit PINX functionality, and also between the transit PINX functionality and the terminating PINX functionality. By definition, the transit PINX functionality will be physically separated from the originating PINX functionality and also the terminating PINX functionality. In other cases functional groupings, e.g. the transit PINX functional grouping and the incoming gateway PINX functional grouping, may also be physically separated and in this case, an IVN and interfaces at the C reference point will exist. However, for simplicity, the figures do not show this case.

The properties of the IVN need to be defined in the case where (some of) the CN functionality is provided by the public network.

A.1.2 Structured overview of the functional groupings which may be involved in a call

Figure A.1 shows all of the functional groupings which may be involved in calls supported by CNs. For a particular call example, some of the functional groupings, e.g. Transit PINX functionality, may be null. In addition, a PINX implementation will contain a number of the functional groupings in the figure, although the functional groupings will not all be used on a call.

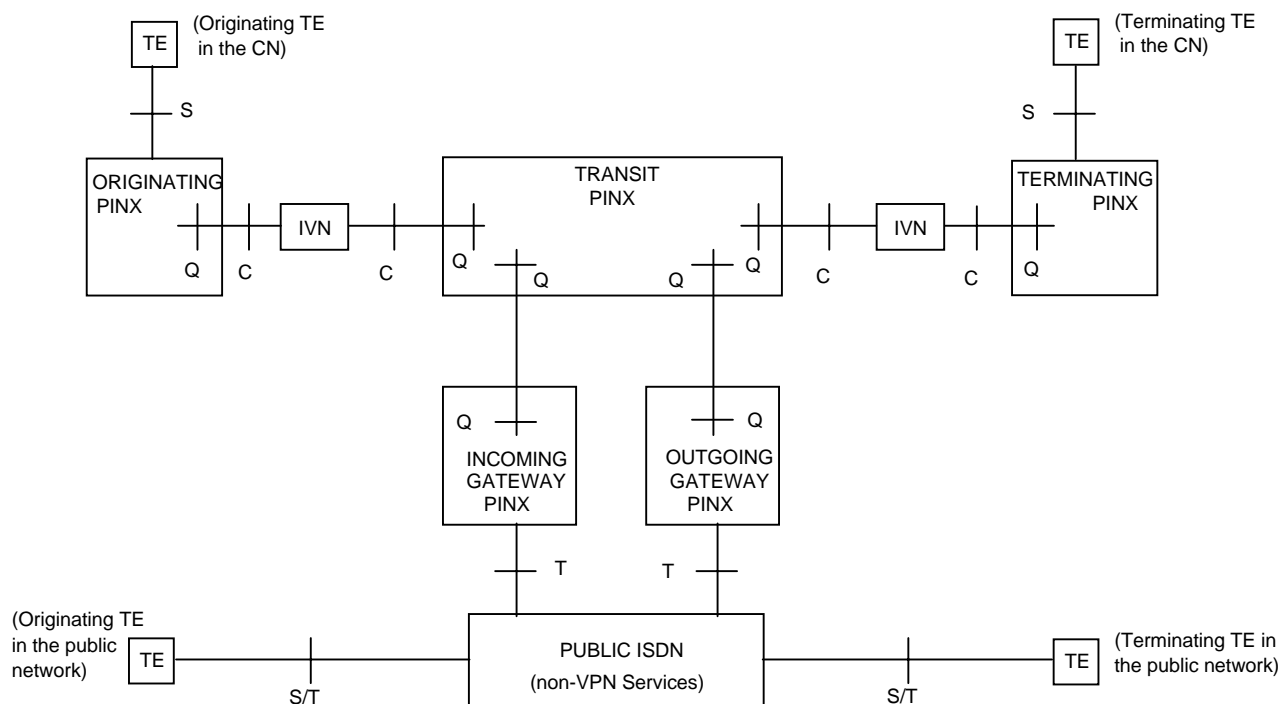


Figure A.1: Structured overview of the functional groupings that may be involved in a CN call

"Public ISDN" shown in figure A.1 represents functionality in the public network other than VPN services for the support of CNs.

The various TEs represent call originating functionality or call terminating functionality for users attached to the CN and users attached to the public network.

Figure A.1 should be read from the left (originating functionality) to the right (terminating functionality) for call examples as follows:

- for a call between two terminals wholly within the CN, the originating terminal is represented by the "originating TE in the CN" and the call passes through an originating PINX, through the CN via transit PINX(s) to the terminating PINX, and then to the "terminating TE in the CN";
- for a call from a terminal connected to the public network to a terminal in the CN (i.e. an incoming call), the originating terminal is represented by the "originating TE in the public network" and the call uses the services of the public network for routing the call to the CN, it enters the CN via the incoming gateway PINX, passes through the CN via transit PINX(s) to the terminating PINX, and then to the "terminating TE in the CN";
- for a call from a terminal within the CN to a terminal connected to the public network (i.e. an outgoing call), the originating terminal is represented by the "originating TE in the CN" and the call passes through an originating PINX, through the CN via transit PINX(s) to the gateway PINX, into the public network and to the "terminating TE in the public network".

Other call scenarios can be constructed. For example, there may be more than one instance of transit PINX functionality on a call (i.e. four or more PINXs are involved in the call) and if the communication link between two of the transit PINXs is congested or out of service, alternative routing mechanisms could route the call via the public network.

Figures A.2 and A.3 are based on figure A.1 and give some examples of which functional groupings could reside in the public network.

NOTE: For simplicity, these examples show functional groupings provided by the public network. This does not preclude functional groupings being provided by third party service providers.

A.1.3 Transit networking service provided by the public network

Figure A.2 contains an example where the transit and gateway functional groupings for calls are provided by the public network. Services provided to the PINX containing the originating PINX functionality and also to the PINX containing the terminating PINX functionality correspond to VPN services applicable to the b service entry point.

The individual functional groupings are shown separately within the group marked "transit networking", but this is not intended to make any recommendations to constrain the implementation. Note also that this example does not preclude physical PBXs within the CN from also performing these functions on some calls.

In this example, the IVN functionality between the originating PINX functionality and the transit PINX functionality, and also between the transit PINX functionality and the terminating PINX functionality shown in figure A.1 is considered to reside in the public network and, as a result this functionality is not shown in figure A.2.

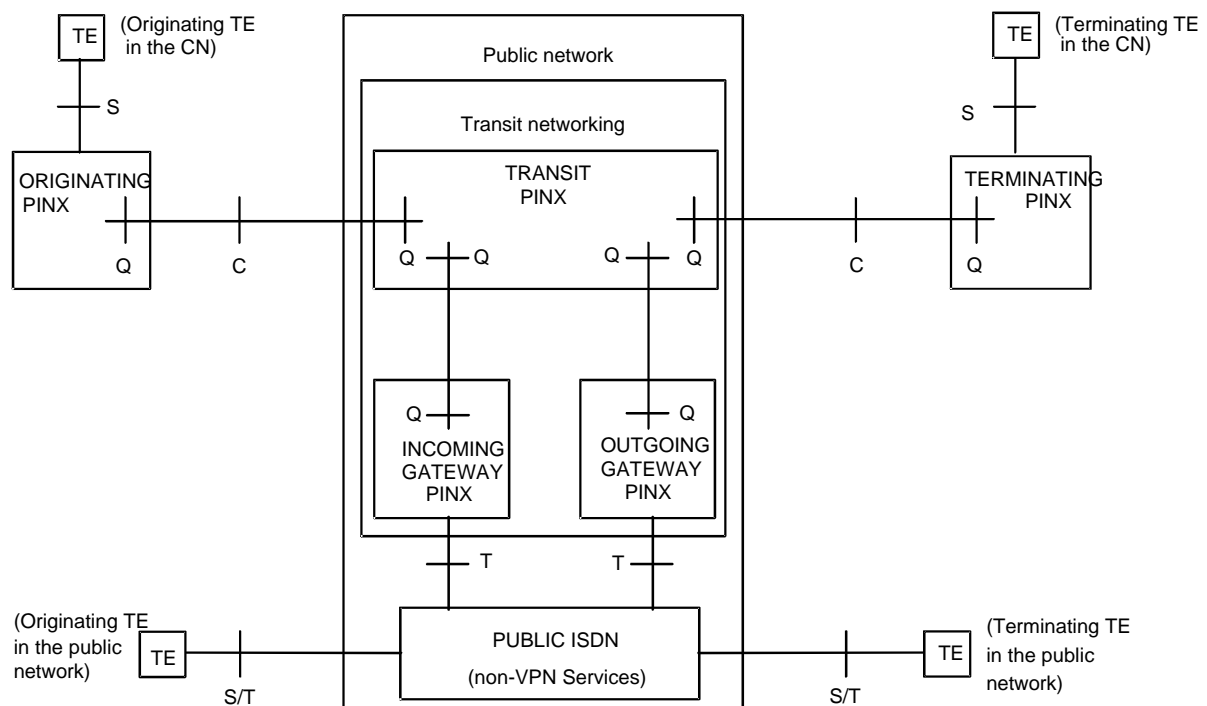


Figure A.2: Transit networking service provided by the public network

A.1.4 Transit and terminating functions provided by the public network

Figure A.3 contains an example where the terminating functional grouping is also provided by the public network. Services provided to the PINX containing the originating PINX functionality correspond to the VPN services applicable to the b service entry point. Services provided to the user at the terminating end of the call correspond to VPN services applicable to the a1 service entry point and the a2 service entry point.

The individual functional groupings are shown separately within the public network, but this is not intended to make any recommendations to constrain the implementation.

In this example, the IVN functionality between the transit PINX and the terminating PINX functional groupings resides in the public network. Also, the IVN functionality between the originating PINX functionality and the transit PINX functionality shown in figure A.2 is considered to reside in the public network and, as a result this functionality is not shown in figure A.3.

In practice, the public network would also provide an originating PINX functional group, but the purpose of the example in figure A.3 is to model calls where the caller is connected to a physical PBX, or public network.

Also, an additional figure could be drawn in order to model calls where the originating PINX functional grouping is provided by the public network and the terminating PINX functional grouping is provided by a physical PBX. In this case, services provided to the user at the originating end of the call correspond to VPN services applicable to the a1 service entry point and services provided to the PINX containing the terminating PINX functionality correspond to VPN services applicable to the b service entry point.

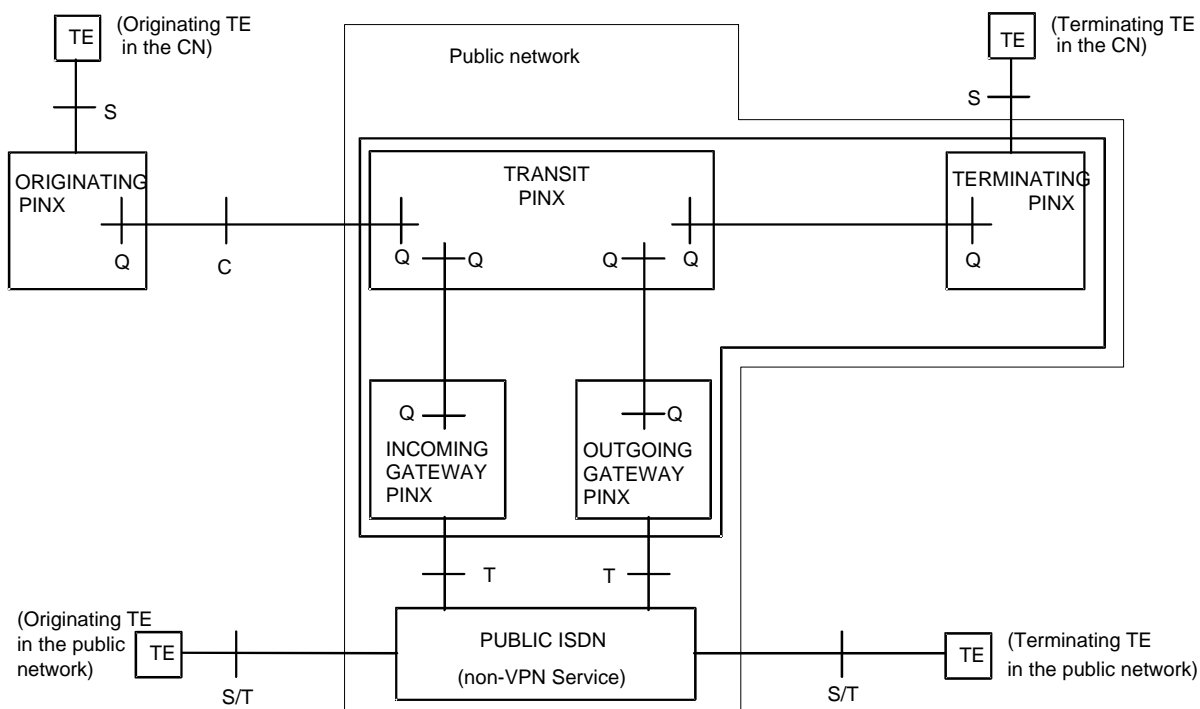


Figure A.3: Transit and terminating functional provided by the public network

Annex B (informative): Relationship between outgoing side and incoming side

Figure B.1 indicates the relationship between "outgoing side" and "incoming side" with respect to the direction of origination of a call and the PINX functionality involved in the call.

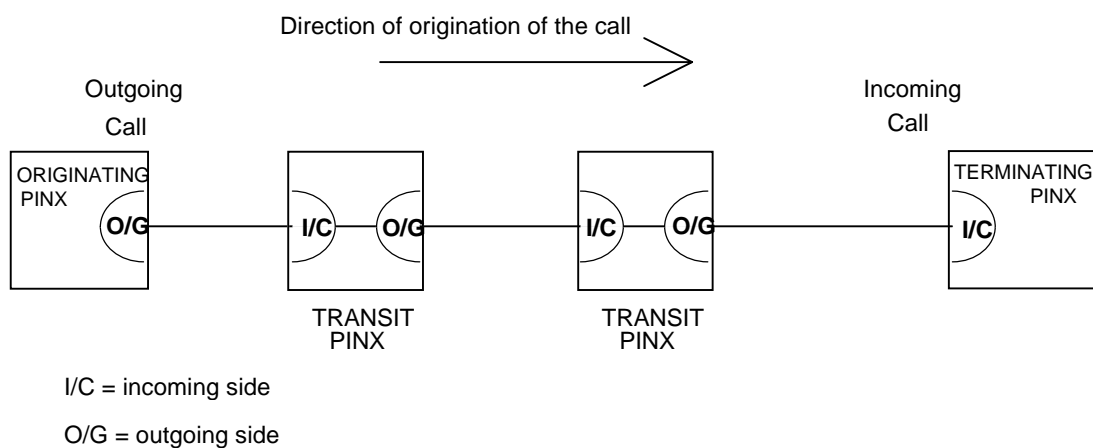


Figure B.1: Definition of incoming and outgoing sides

History

Document history			
V1.1.1	August 1997	Public Enquiry	PE 9748: 1997-08-01 to 1997-11-28