Final draft EN 301 060-1 V1.2.2 (1998-01)

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 (9tc90ipc.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

Contents

Intellectual Property Rights

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

Pursuant to the ETSI Interim IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETR 314 (or the updates on http://www.etsi.fr/ipr) which are, or may be, or may become, essential to the present document.

Foreword

This European Standard (Telecommunications series) has been produced by ETSI Technical Committee Signalling Protocols and Switching (SPS), and is now submitted for the Voting 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 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 specifies the extensions of the protocol for basic call control for the pan-European Integrated Services Digital Network (ISDN). These extensions are applicable at the "b" service entry point (as defined in clause 5 of the present document). It is part of the Digital Subscriber Signalling System No. One (DSS1) protocol. The present document contains only additional requirements to those in the main body of ETS 300 403-1 [2].

The present document is applicable only to point-to-point access configurations.

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

- the emulation of an Originating Private Integrates services Network Exchange (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 "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 EN 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] EN 300 403-1: "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 (1994): "Information technology -- Telecommunications and information exchange between systems -- Numbering and sub-addressing in private integrated services networks".

[7] ISO/IEC 11572 (1996), plus Amendment 1 (1996) and Amendment 2 (1996): "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 11579-1 (1994): "Information technology -- Telecommunications and information exchange between systems -- Private integrated services network -- Part 1: Reference configuration for PISN Exchanges (PINX)".

[9] ISO/IEC 15056 (1997): "Information technology - Telecommunications and information exchange between systems - Private Integrated Services Network - Inter-exchange signalling protocol - Transit counter additional network feature".

2.2 Informative references

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

[11] ETR 172 second edition (1995): "Business TeleCommunications (BTC); Virtual Private Networking (VPN); Services and networking aspects; Standardization requirements and work items".

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 to 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 CN.

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 CN to other networks.

preceding PINX: In the context of a call, an entity with PINX functionality located in the direction towards the originating interface. A preceding PINX may be functionality provided by a physical PINX or may be an emulation of PINX functionality by the public network.

Private Integrated services Network eXchange (PINX): A PISN nodal entity that provides automatic switching and call handling functions used for the provision of telecommunication services. 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 identifies calls between users in the CN, and relays such calls to designated PINX functionality emulated by the public network, 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.

subsequent PINX: In the context of a call, an entity with PINX functionality located in the direction towards the destination interface. A subsequent PINX may be functionality provided by a physical PINX or may be an emulation of PINX functionality by the public network.

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): 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-TC	Additional Network Feature - Transit Counter
BCD	Binary Coded Digit
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
IVN	InterVening Network
ISDN	Integrated Services Digital Network
LAN	Local Area Network
PBX	Private Branch eXchange
PINX	Private Integrated services 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 EN 300 403-1 [2] to support calls within a Corporate telecommunication Network (CN) and to support calls which enter or exit the CN via Gateway Private Integrated services Network eXchange (PINX) functionality performed by the public network. 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 (providing 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 or may be an emulation of an End PINX functionality provided by the public network.

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.

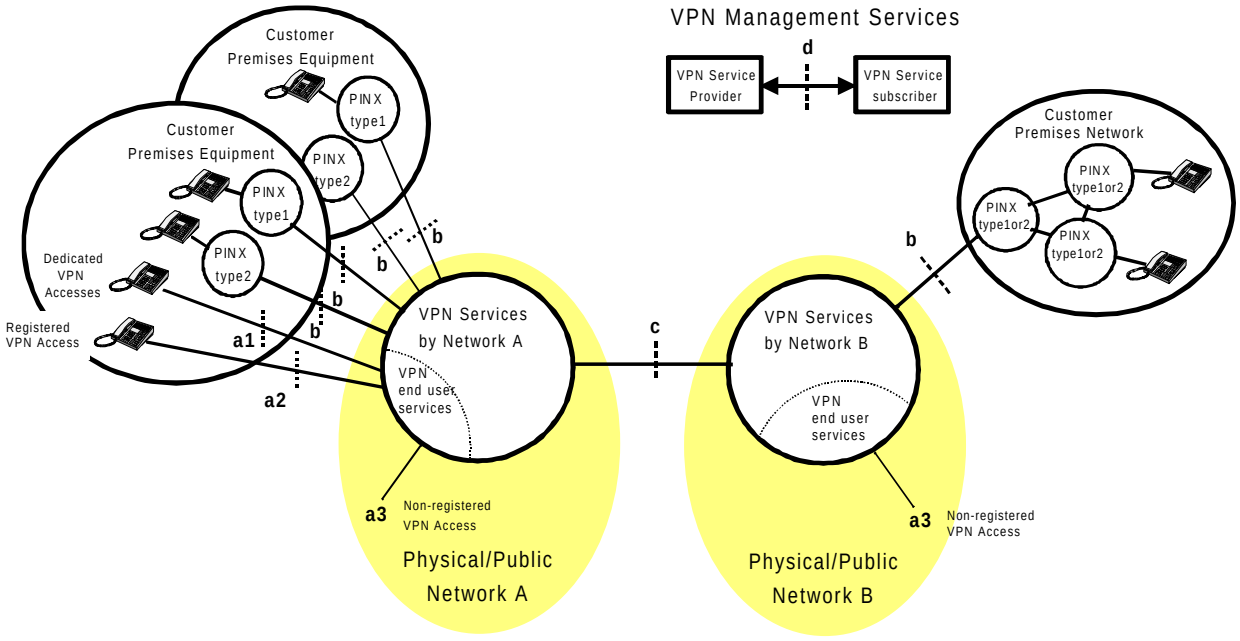
The following PINX types are defined:

PINX type 1: An implementation of a PINX outside the public network that supports services provided by the public ISDN and/or PSTN.

PINX type 2: An implementation of a 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.

The "a1", "a2", and "a3" service entry points are subcategories of the "a" service entry point that provides VPN end-user services.

5.2 Networking aspects - requirements

The public network 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.

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.

For the emulation of Transit PINX functionality, the functions provided by the public network 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 (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 transit counter additional network feature (ANF-TC) defined in ISO/IEC 15056 [9] may be supported by those extensions to the DSS1 protocol.

For the emulation of Incoming Gateway PINX functionality, the functions provided by the public network 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 ANF-TC defined in ISO/IEC 15056 [9] 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 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 ANF-TC defined in ISO/IEC 15056 [9] may be supported by those extensions to the DSS1 protocol.

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 different CNs. Thus, the virtual transit PINX or virtual gateway PINX need 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 routeing 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.

The capability of supporting multiple CNs is fulfilled by the VPN indicator information element 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.

For the emulation of Originating PINX functionality, the functions provided by the public network 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 (CLIP, CLIR, COLP, COLR, SUB). In addition ANF-TC defined in ISO/IEC 15056 [9] may be supported by those extensions to the DSS1 protocol.

For the emulation of Terminating PINX functionality, the functions provided by the public network 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 ANF-TC defined in ISO/IEC 15056 [9] may be supported by those extensions to the DSS1 protocol.

The requirements identified here are not required in every switching element in the public network.

5.2.3 Provision of Relay Node functionality in the public network

For Relay Node functionality, the public network shall provide:

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

5.2.4 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 PINXs.

6 Operational requirements

The provision of the capabilities described in the present document may require a prior arrangement between the operator of the physical PINX and the public network infrastructure.

The public network infrastructure shall be able to associate one CN with the access, and may as an option be able to associate multiple CNs with the access.

As an option, the operator of the public network infrastructure may offer the VPN service with the subscription option shown in table 1. This option shall apply per access.

Table 1

Option	Values
Default CN	Nominated CN, or none designated

7 Coding requirements

The coding requirements in this clause apply to the VPN context. The coding requirements applicable to the public network context are outside the scope of the present document.

NOTE 1: The coding of messages and information elements relating to the restart procedures in EN 300 403-1 [2] apply regardless of the context, i.e. they are common to both the public network context and the VPN context.

NOTE 2: The coding of messages and information elements relating to the segmentation and reassembly procedures in EN 300 403-1 [2] apply regardless of the context, i.e. they are common to both the public network context and the VPN context.

7.1 Additional messages and content

The coding requirements contained in subclause 3.1 of EN 300 403-1 [2] relating to the ALERTING, CALL PROCEEDING, CONNECT ACKNOWLEDGE, PROGRESS, SETUP ACKNOWLEDGE, DISCONNECT, RELEASE, RELEASE COMPLETE, INFORMATION, STATUS and STATUS ENQUIRY messages shall apply unchanged in a VPN context.

The coding requirements contained in subclause 3.1 of EN 300 403-1 [2] relating to the CONNECT and SETUP messages shall apply in a VPN context with the additions specified in the following subclauses.

NOTE: The NOTIFY message forms part of the basic call in a public network context. However, in a VPN context it forms part of the Generic Functional Protocol for the support of supplementary services.

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

The coding requirements contained in subclause 3.1 of EN 300 403-1 [2] relating to the following information elements shall apply unchanged in a VPN context:

- Locking shift;
- Non-locking shift;
- Sending complete;
- Bearer capability;
- Cause;
- Call state;
- Channel identification;
- Calling party subaddress;
- Called party subaddress;
- Low layer compatibility; and
- High layer compatibility.

The coding requirements contained in subclause 3.1 of EN 300 403-1 [2] relating to the following information elements shall apply in a VPN context with the additions specified in the following subclauses:

- Progress indicator;
- Calling party number; and
- Called party number.

The following information elements are additional to those contained in subclause 3.1 of EN 300 403-1 [2]:

- Connected number;
- Connected subaddress;
- Transit counter; and
- VPN indicator.

NOTE: The Notification indicator information element forms part of the basic call in a public network context. However, in a VPN context it forms part of the Generic Functional Protocol for the support of supplementary services.

7.2.1 Called party number

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

Table 2: 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 field 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 [10].
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 3) when Numbering Plan identification is Unknown

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 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 (note 7)
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.
NOTE 7: The type of number "unknown" is used when the user or the network has no knowledge of the type of number, e.g. Level 1, Level 2, 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.

Number digits (octets 4, etc.)

This field is 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 EN 300 403-1 [2] shall apply with the exception that table 4.11 of EN 300 403-1 [2] is replaced by the following table:

Table 3: Calling 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 field 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 Recommendation I.330 [10].
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.

Type of number (octet 3) when Numbering Plan identification is Unknown

```
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.

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

```
Bits
7  6  5
0  0  0     Unknown (note 7)
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.
NOTE 7: The type of number "unknown" is used when the user or the network has no knowledge of the type of number, e.g. Level 1, Level 2, 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.

(continued)

Table 3 (concluded): Calling party number

Presentation indicator (octet 3a)

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

Screening indicator (octet 3a)

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

Number digits (octets 4, etc.)

This field is 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

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 coding of the Transit counter information element is defined in ISO/IEC 15056 [9].

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 include a CN identifier to distinguish between CNs in the VPN environment, i.e. the combination of the CN indicator and CN identifier values uniquely identify the CN. The VPN indicator information element shall have a maximum length of 15 octets.

The VPN indicator information element is defined in codeset 0.

The VPN indicator information element is coded as shown in figure 2, and table 4.

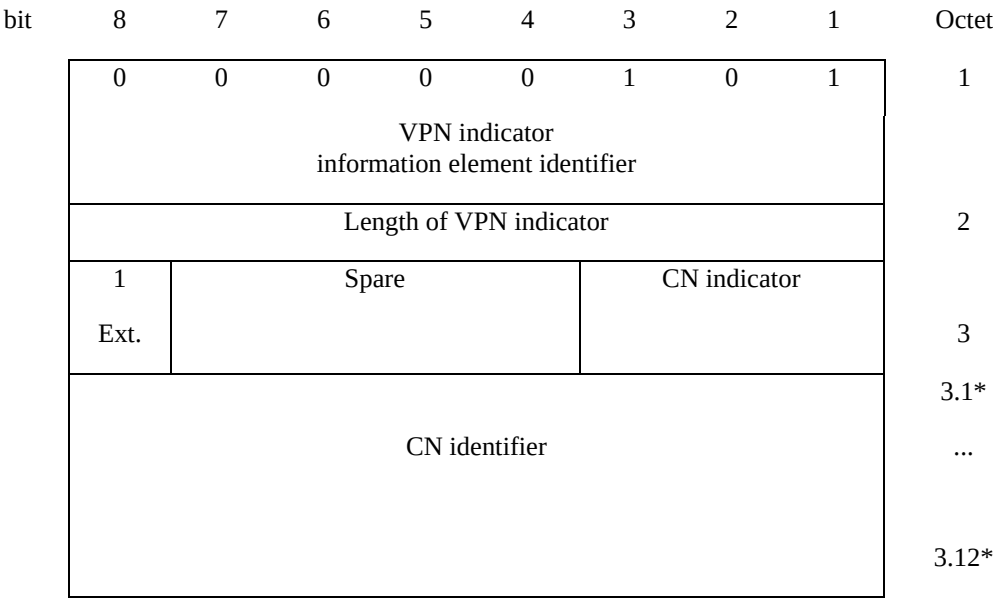


Figure 2: VPN indicator information element

Table 4: VPN indicator

CN indicator (octet 3)

```
Bits
3  2  1
0  0  0     no indication (note 1)
0  0  1     network specific(note 2)
0  1  0     global (note 3)
```

All others values are reserved.

NOTE 1: When the CN indicator "no indication" is used, the call belongs to the assigned default CN.
NOTE 2: When the CN indicator "network specific" is used, the CN identifier is contained in the octets 3.1 to 3.12. This value only has significance within the public network to which the user is attached.
NOTE 3: When the CN indicator "global" is used, the CN identifier in octets 3.1 to 3.12 following contains a globally unique value.

CN identifier (octets 3.1 to 3.12)

When the CN indicator is set to "no indication", no CN identifier shall be included.

When the CN indicator is set to "network specific", the coding of the CN identifier is a network provider matter.

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

8 Basic call states

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

9 Circuit-switched call control procedures

NOTE 1: The restart procedures in EN 300 403-1 [2] apply regardless of the context, i.e. they are common to both the public network context and the VPN context.

NOTE 2: The segmentation and reassembly procedures in EN 300 403-1 [2] apply regardless of the context, i.e. they are common to both the public network context and the VPN context.

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 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.

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.

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 EN 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 EN 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 at the originating interface shall include the VPN indicator information element in the SETUP message.

If the public network receives a SETUP message with a VPN indicator information element that does not contain a CN identifier and a CN identifier is registered as a default for the access, then the default CN identifier shall be used.

If the public network receives SETUP message with a VPN indicator information element that does not contain a CN identifier and there is no CN identifier registered as a default for the access, then the call shall be rejected with cause #50 "requested facility not subscribed".

If the public network receives a SETUP message with a VPN indicator information element that indicates a CN which is not associated with the access, then the call shall be rejected with cause #50 "requested facility not subscribed".

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

If received from the physical PINX at the originating interface, 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 subsequent PINX, regardless of any supplementary service subscription information;
- a Relay Node shall transfer the information elements to the subsequent PINX regardless of 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;
- a Terminating PINX may transfer the information elements to the called user, depending on any restrictions (e.g. interface type or service).

NOTE: The handling of numbers by an Outgoing Gateway PINX, e.g. translations, presentation indications, is outside the scope of the present document. If the received Calling party number information element has the presentation indicator value "presentation restricted", presentation of the number to the other network will depend on such factors as the other network's commitment to honour the restriction.

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

- a Transit PINX shall transfer the information element to the subsequent PINX;
- a Relay Node shall transfer the information element to the subsequent PINX;
- 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 called user.

Refer to subclause 9.3.3 for procedures relating to the notification of interworking and provision of in-band information.

9.3.1.2 Call confirmation

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

- if received from a subsequent PINX, a Transit PINX shall transfer the information elements towards the physical PINX at the originating interface, regardless of any possible supplementary service subscription information;
- if received from a subsequent PINX, a Relay Node shall transfer the information elements towards the physical PINX at the originating interface, regardless of 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 CN; and
- a Terminating PINX shall provide (or complete any partial information received from the connected user) the Connected number information element towards the physical PINX at the originating interface, regardless of any possible service subscription information. Furthermore, a Terminating PINX shall transfer the Connected subaddress information element if received from the connected user, regardless of any possible service subscription information.

NOTE: The handling of numbers by an Outgoing Gateway PINX, e.g. translations, presentation indications, is outside the scope of the present document.

9.3.2 Establishment of calls towards a physical PINX

9.3.2.1 Incoming call

The public network shall include the VPN indicator information element in the SETUP message. The public network shall include a CN identifier in the VPN indicator information element.

If the PINX receives a SETUP message and can determine that the CN identifier is not associated with the access, then the call shall be rejected with cause #50 "requested facility not subscribed".

Incoming Gateway PINX functionality and Originating PINX functionality shall generate the VPN indicator information element (e.g. as a result of a fixed relationship between a terminal at the "a" service entry point and the CN to which it belongs) if the information is not already available.

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

- if received from a preceding PINX, a Transit PINX shall transfer the information elements towards the physical PINX at the destination interface, regardless of any supplementary service subscription information;
- if received from a preceding PINX functionality, a Relay Node shall transfer the information elements towards the physical PINX at the destination interface, regardless of 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 CN; and
- an Originating PINX shall generate (or complete any partial information received from the calling user) the Calling party number information element towards the physical PINX at the destination interface, regardless of any possible service subscription information. Furthermore, an Originating PINX shall transfer the Calling party subaddress information element if received from the calling user, regardless of any possible service subscription information.

NOTE: The handling of numbers by an Incoming Gateway PINX, e.g. translations, presentation indications, is outside the scope of the present document.

The public network shall include the Transit counter information element in the SETUP message if received from the preceding PINX.

Refer to subclause 9.3.3 for procedures relating to the notification of interworking and provision of in-band information.

9.3.2.2 Call confirmation

The physical PINX at the destination interface 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 at the destination interface in the CONNECT message, shall be transferred by the public network as follows:

- a Transit PINX shall transfer the information elements towards the preceding PINX, regardless of any supplementary service subscription information;
- a Relay Node shall transfer the information elements towards the preceding PINX, regardless of 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. If the CONNECT message contains a Connected subaddress information element, then if the information element can be conveyed to the other network, it shall be conveyed unchanged; and
- an Originating PINX may transfer the information elements to the calling user, depending on any restrictions.

NOTE: The handling of numbers by an Incoming Gateway PINX, e.g. translations, presentation indications, is outside the scope of the present document. If the received Connected number information element has the presentation indicator value "presentation restricted", presentation of the number to the other network will depend on such factors as the other network's commitment to honour the restriction.

9.3.3 Notification of interworking and provision of in-band information

The following subclauses document notification of interworking and requirements to connect through in order to provide in-band information. Since the requirements are common to the entities at either side of an originating interface and the entities at either side of a destination interface, the requirements are structured from the point of view of:

- a preceding PINX, i.e. a physical PINX at the originating interface or public network at the destination interface; and
- a subsequent PINX, i.e. a physical PINX at the destination interface or public network at the originating interface.

9.3.3.1 Actions at a preceding PINX

The usage and handling of the Progress indicator information element depends on the type of nodal functionality.

a) A Transit PINX shall act as follows:

   - a Transit PINX shall transfer a received Progress indicator information element unchanged to the subsequent PINX;
   - if a Transit PINX receives an ALERTING or PROGRESS message with progress description values #1 "call is not end-to-end ISDN, further information may be available in-band", or #8 "in-band information or appropriate pattern now available", the allocated information channel shall be connected through in the backward direction, if this has not already occurred;
   - a Transit PINX shall generate progress description value #8 "in-band information or appropriate pattern now available" if it generates a tone or an announcement; and
   - a Transit PINX shall support the handling of additional progress descriptions in accordance with ZB.1, ZB.2 and ZB.4 in Annex ZB of Amendment 1 to ISO/IEC 11572 [7].

b) An Originating PINX shall handle the Progress indicator information element as specified in the following subclauses of ISO/IEC 11572 [7]:

   - subclause 10.5.1, item b) - sending in the SETUP message;

- subclause 10.5.3 - receipt in PROGRESS, ALERTING and CONNECT messages;
- subclause 10.5.4 - receipt in the ALERTING message;
- subclause 10.5.6, 2nd paragraph - abandoning a call; and
- Annex ZB of Amendment 2 - ZB.1, ZB.3, and ZB.7 - additional progress descriptions.

c) An Incoming Gateway PINX shall handle the Progress indicator information element as specified in the following subclauses of ISO/IEC 11572 [7]:

- subclause 10.7.2 - sending in the SETUP message;
- subclause 10.7.4 - receipt in PROGRESS, ALERTING and CONNECT messages;
- subclause 10.7.5, 2nd paragraph - abandoning a call; and
- Annex ZB of Amendment 2 - ZB.1, ZB.3, and ZB.5 - additional progress descriptions.

d) A Relay Node shall act as follows:

- a Relay Node shall transfer a received Progress indicator information element unchanged to the next entity with PINX functionality;
- if a Relay Node receives an ALERTING or PROGRESS message with progress description values #1 "call is not end-to-end ISDN, further information may be available in-band", or #8 "in-band information or appropriate pattern now available", the allocated information channel shall be connected through in the backward direction, if this has not already occurred;
- a Relay Node shall generate progress description value #8 "in-band information or appropriate pattern now available" if it generates a tone or an announcement; and
- a Relay Node shall support the handling of additional progress descriptions in accordance with ZB.1 and , ZB.2 in Annex ZB of Amendment 1 to ISO/IEC 11572 [7].

9.3.3.2 Actions at a subsequent PINX

The usage and handling of the Progress indicator information element depends on the type of nodal functionality.

a) A Transit PINX shall act as follows:

- a Transit PINX shall transfer a received Progress indicator information element unchanged to the subsequent PINX;
- if a Transit PINX receives an ALERTING or PROGRESS message with progress description values #1 "call is not end-to-end ISDN, further information may be available in-band", or #8 "in-band information or appropriate pattern now available", the allocated information channel shall be connected through in the backward direction, if this has not already occurred;
- a Transit PINX shall generate progress description value #8 "in-band information or appropriate pattern now available" if it generates a tone or an announcement; and
- a Transit PINX shall support the handling of additional progress descriptions in accordance with ZB.1, ZB.2 and ZB.4 in Annex ZB of Amendment 1 to ISO/IEC 11572 [7].

b) A Terminating PINX shall handle the Progress indicator information element as specified in thef following subclauses of ISO/IEC 11572 [7]:

- subclause 10.6.1, item a) - receipt in the SETUP message;
- subclause 10.6.2 - sending in the ALERTING message;
- subclause 10.6.3 - sending in PROGRESS, ALERTING and CONNECT messages;
- subclause 10.6.5, 2nd paragraph - abandoning a call; and

- Annex ZB of Amendment 2 - ZB.1, ZB.3, and ZB - additional progress descriptions.

c) An Outgoing Gateway PINX shall handle the Progress indicator information element as specified in thefollowing subclauses of ISO/IEC 11572 [7]:

- subclause 10.8.1 item a) - receipt in the SETUP message;
- subclause 10.8.3 - sending in PROGRESS, ALERTING and CONNECT messages;
- subclause 10.8.4 2nd paragraph - sending in the ALERTING message;
- subclause 10.8.6, 2nd paragraph - abandoning a call; and
- Annex ZB of Amendment 2 - ZB.1, ZB.3, and ZB.6 - additional progress descriptions.

d) A Relay Node shall act as follows:

- a Relay Node shall transfer a received Progress indicator information element unchanged to the next entity with PINX functionality;
- if a Relay Node receives an ALERTING or PROGRESS message with progress description values #1 "call is not end-to-end ISDN, further information may be available in-band", or #8 "in-band information or appropriate pattern now available", the allocated information channel shall be connected through in the backward direction, if this has not already occurred;
- a Relay Node shall generate progress description value #8 "in-band information or appropriate pattern now available" if it generates a tone or an announcement; and
- a Relay Node shall support the handling of additional progress descriptions in accordance with ZB.1 and , ZB.2 in Annex ZB of Amendment 1 to ISO/IEC 11572 [7].

10 System parameters

T310: the value of this timer when started or restarted upon receipt of progress description values #1 "call is not end-to-end ISDN, further information may be available in-band" or #8 "in-band information or appropriate pattern now available" 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 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 ETR 172 [11] 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 InterVening Network (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.

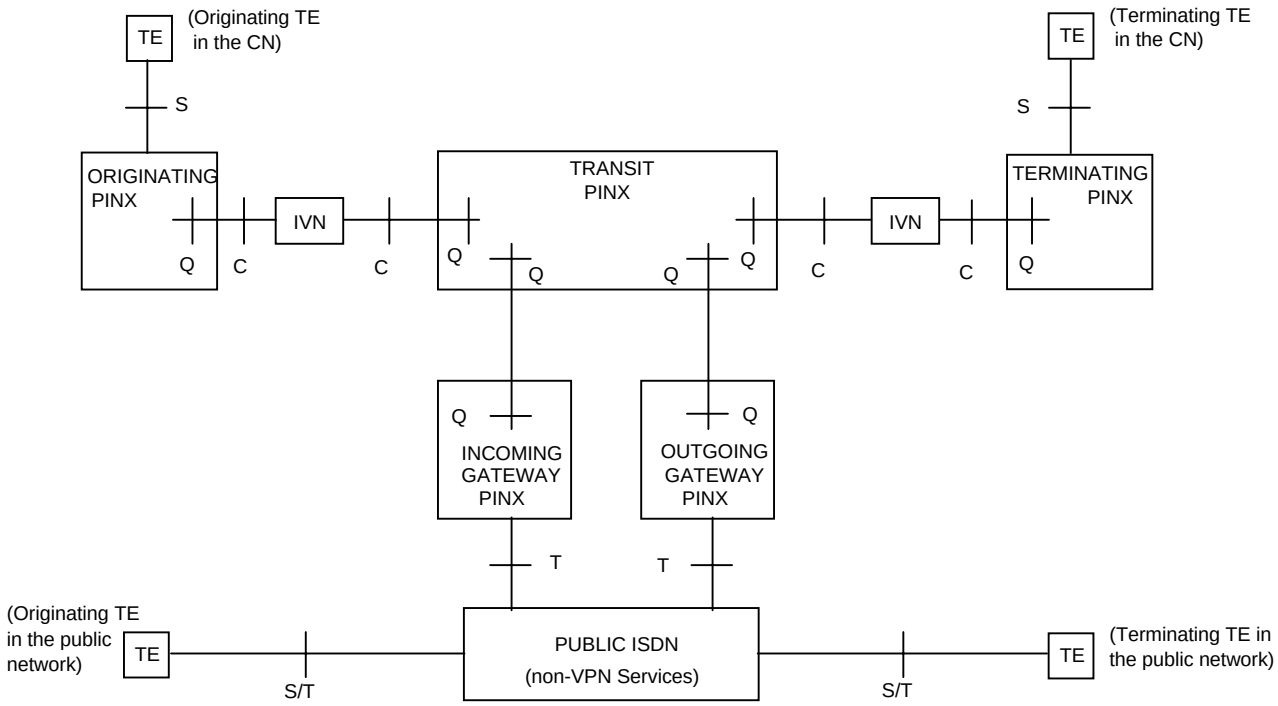


Figure A.1: Structured overview of the functional groupings that may be involved in a CN call

"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 routeing 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 though an Originating PINX, through the CN via Transit PINX(s) to the Outgoing 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 routeing 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 PINXs 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.

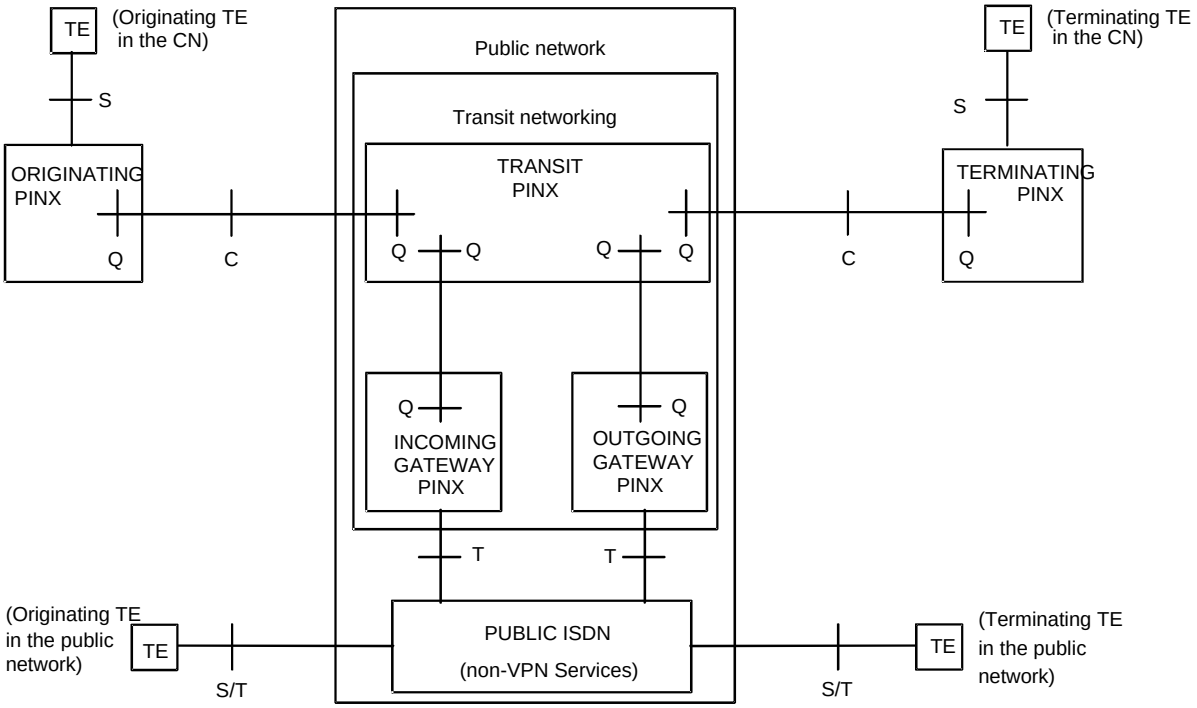


Figure A.2: Transit networking service provided by the public network

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 PINX, 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 PINX. 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.

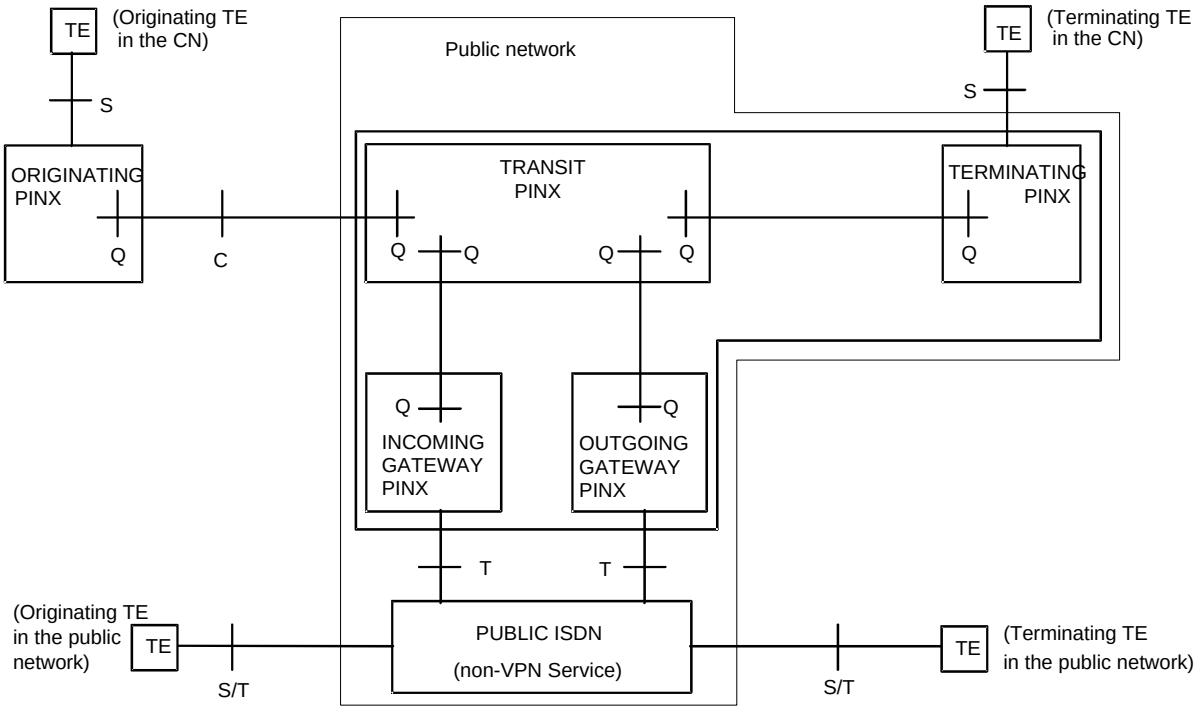


Figure A.3: Transit and terminating functions provided by the public network

History

Document history				
V1.1.1	August 1997	Public Enquiry	PE 9748:	1997-08-01 to 1997-11-28
V1.2.2	January 1998	Vote	V 9813:	1998-01-27 to 1998-03-27