ETSI TECHNICAL COMMITTEE REFERENCE TECHNICAL REPORT

TCR-TR 034

September 1995

Source: ETSI TC-BTC

Reference: DTR/BTC-00006

ICS: 33.020

Key words: VPN, PTN, service, planning

Business TeleCommunications (BTC); Virtual Private Networking (VPN); Services and networking aspects; Standardization requirements and work items

ETSI

European Telecommunications Standards Institute

ETSI Secretariat

Postal address: F-06921 Sophia Antipolis CEDEX - FRANCE
Office address: 650 Route des Lucioles - Sophia Antipolis - Valbonne - FRANCE
X.400: c=fr, a=atlas, p=etsi, s=secretariat - **Internet:** secretariat@etsi.fr

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

Contents

Blank page

Foreword

This Technical Committee Reference Technical Report (TCR-TR) has been produced by the Joint Task Group (JTG) on Virtual Private Networking of the European Telecommunications Standards Institute (ETSI).

JTG/VPN was constituted by representatives from Technical Committee (TC) Business TeleCommunications (BTC), European Computer Manufacturers Association (ECMA), TC Network Aspects (NA) and TC Signalling Protocols and Switching (SPS) besides the ETSI member representatives under the lead of TC BTC.

A TCR-TR is a deliverable for use inside ETSI which records output results of ETSI TC or STC studies which are not appropriate for European Telecommunication Standard (ETS), Interim European Telecommunication Standard (I-ETS) or ETSI Technical Report (ETR) status. They can be used for guidelines, status reports, co-ordination documents, etc.. They are to be used to manage studies inside ETSI and shall be mandatorially applied amongst the concerned TCs. They shall also be utilised by the TC with overall responsibility for a study area for co-ordination documents (e.g. models, reference diagrams, principles, structures of standards, framework and guideline documents) which constitute the agreed basis for several, if not all, TCs and STCs to pursue detailed standards.

NOTE: The content of this TCR-TR has also been published as ETR 172 in order to make it publicly available.

Introduction

This TCR-TR has been produced by an ETSI Joint Task Group in response to a request by users to investigate the impact on standardization activities in the relevant committees of ETSI and ECMA with regard to the subject of VPN based upon recommendations from Strategic Review Committees (SRCs) 4 and 5.

In the context of this study, the treatment of definitions, services and network architecture is primarily considered in terms of Private Branch Exchange (PBX) technology and functionality. This TCR-TR identifies work items that are intended to provide an early solution for the standardization of VPNs that, as minimum, support the interconnection of PBXs. The work items contain standardization requirements for VPN services including:

a) VPN end user services;
b) VPN networking services;
c) inter-VPN services;
d) VPN management services.

Blank page

1 Scope

This ETSI Technical Report (TCR-TR) investigates aspects of Virtual Private Network (VPN) services in the context of Corporate telecommunication Networks (CNs) and identifies work items to be studied by the relevant ETSI Technical Committees (TCs). These work items contain standardization requirements for VPN services including:

a) VPN end-user services;
b) VPN networking services;
c) inter-VPN services;
d) VPN management services.

The scope of the investigation has been limited to the following areas:

- the definition of standardization requirements for VPN services from the perspective of fixed public networks (see the note below);

- the definition of standardization requirements for circuit-mode basic services and supplementary services based upon the concepts of VPN services including Centrex and Private Branch eXchange (PBX) functions.

  NOTE: It should be noted that, mobile networks, data networks, broadband networks and other public networks are all suitable for supporting VPN services. These areas are recommended for further study by the relevant TCs (see annex F).

This TCR-TR identifies a set of core services (within the Class II categorized VPN services[1)] as defined by ETSI/TA18(93)25 [15]) needed for the efficient support of CNs and recommends standardization activities to meet these service requirements.

This TCR-TR assumes and maintains the traditional distinction between public and private networks. However, it is recognized that the European Commission (EC) is currently investigating service liberalization which in the near future may lead to break down this distinction. This may ultimately impact technical standardization work to be undertaken on VPN services and it may be appropriate for ETSI to seek EC guidance in these matters.

The mission statement for the Joint Task Group is presented in annex G.

2 References

For the purposes of this TCR-TR, the following references apply:

[1] ETS 300 171 (1992): "Private Telecommunication Network (PTN); Specification, functional models and information flows; Control aspects of circuit mode basic services".

[2] ETS 300 190 (1992): "Private Telecommunication Network (PTN); Signalling at the S-reference point; Generic keypad protocol for the support of supplementary services".

[3] ETS 300 191 (1992): "Private Telecommunication Network (PTN); Signalling protocol at the S-reference point; Identification supplementary services".

[4] ETS 300 192 (1992): "Private Telecommunication Network (PTN); Signalling protocol at the S-reference point; Circuit mode basic services".

[5] ETS 300 239 (1993): "Private Telecommunication Network (PTN); Inter-exchange signalling protocol; Generic functional protocol for the support of supplementary services".

---

1) Class II category is defined in ETSI/TA18 (93) 25 [15] as CPE/CPN to VPN services to CPE/CPN.

[6] ETS 300 345 (1994): "Integrated Services Digital Network (ISDN); Interworking between public ISDNs and private ISDNs for the provision of telecommunication services; General aspects".

[7] ETS 300 415: "Private Telecommunication Network (PTN); Terms and definitions".

[8] ETS 300 475-1: "Private Telecommunication Network (PTN); Reference configuration; Part 1: Reference configuration for PTN eXchanges (PTNXs) [ISO/IEC 11579-1 (1994), modified]".

[9] ETR 076: "Integrated Services Digital Networks (ISDN); Standards guide".

[10] ETR 146 (1994): "Private Telecommunication Network (PTN); Private Telecommunication Network Exchange (PTNX) functions for the utilization of intervening networks in the provision of overlay scenarios (transparent approach); General requirements".

[11] TCR-TR 024: "ISDN Management and Co-ordination Committee; Public and private ISDN service harmonisation".

[12] TCR-TR 027: "Intelligent Network (IN); Vocabulary of terms and abbreviations".

[13] TCR-TR 033: "Private Telecommunication Network (PTN); Integrated scenario for business communications".

[14] ETSI/TA14(92)29: "Strategic Review Committee on the Public Network Infrastructure (SRC4): Report to the Technical Assembly".

[15] ETSI/TA18(93)25: "Strategic Review Committee on Corporate Telecommunications Networks (SRC5): Report to the Technical Assembly".

[16] CCITT Recommendation X.219 (1988): "Remote operations: Model, notation and service definition".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of this TCR-TR, the following definitions apply:

C reference point: Defines the boundary between the mapping functional grouping and the InterVening Network (IVN). The physical, electrical and procedural interface characteristics shall be specified at this reference point, as well as the signalling information flows which are necessary for the control of the inter PTNX connections provided by the IVN. (See ETS 300 475-1 [8]).

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. (See ETSI/TA18(93)25 [15]).

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

NOTE 2: In this TCR-TR, even equipment which is not geographically dispersed (e.g., a single PBX or a Centrex providing service to users at a single location) may form a CN.

CN administrator: An authority responsible for the provision and management of a CN.

CN user: A user who is a member of a CN.

gateway PTNX functionality: This provides functionality to support access to another network, be it the public network, or another CN. Gateway PTNX functionality can be further subdivided into "incoming

gateway PTNX" functionality which supports calls entering the CN, and "outgoing gateway PTNX" functionality which supports calls which exit the CN. (See ETS 300 415 [7]).

NOTE 3: This functional grouping is a logical grouping and place no constraints on the physical implementation, e.g. the location of the functionality. Also, it is not constrained to any particular network architecture, e.g. the functionality of a functional group may be distributed across the network, or located at a single place. The relationship between, and the flow of information between functional groupings does not imply the use of any particular protocol.

originating PTNX functionality: Provides functionality to support calls from the calling user, e.g. analysis of the dialled number and checks on the calling user's class of service. Originating PTNX functionality is a subset of end PTNX functionality defined in ETS 300 415 [7].

NOTE 4: This functional grouping is a logical grouping and place no constraints on the physical implementation, e.g. the location of the functionality. Also, it is not constrained to any particular network architecture, e.g. the functionality of a functional group may be distributed across the network, or located at a single place. The relationship between, and the flow of information between functional groupings does not imply the use of any particular protocol.

Private Telecommunication Network eXchange (PTNX): A Private Telecommunication Network (PTN) nodal entity that provides automatic switching and call handling functions used for the provision of telecommunication services. A nodal entity consists of one or more nodes. The nodal entity, performing the functions outlined above, can be implemented by equipment located on the premises of the private network administrator or by equipment collocated with, or physically part of, a public network. (See ETS 300 415 [7]).

A PTNX may perform the functions of one or more of the following node types:

- telecommunication services within its own area; and/or
- telecommunication services from the public Integrated Services Digital Network (ISDN); and/or
- telecommunication services from other public or private networks; and/or
- within the context of a PTN, telecommunication services from other PTNXs to users of the same and/or other PTNXs.

Q reference point: The Q reference point defines the boundary between the switching and mapping functional groupings in the PTNX reference configuration. The inter PTNX call control functions and signalling information flows shall be specified at this reference point. (See ETS 300 475-1 [8]).

Q interface SIGnalling protocol (QSIG): Generic name describing signalling information flows (i.e., not a specific signalling protocol), within a D_Q-channel. (See ETR 146 [10]).

NOTE 5: The D_Q-channel is used to convey call control information between Q reference points of two peer PTNXs.

service entry point: Indicates where VPN services are presented without reference to any specific protocol or interface to be used.

service provider: An actor who provides services to its subscribers on a contractual basis and who is responsible for the services offered. The same organization may act as a network operator and as a service provider. (See TCR-TR 027 [12]).

service subscriber: An entity that contracts for services offered by service providers. (See TCR-TR 027 [12]).

terminating PTNX functionality: Provides functionality to support calls to the called user, e.g. checking the called user's state (free, busy, etc.) and checks on the called user's class of service. Terminating PTNX functionality is a subset of end PTNX functionality defined in ETS 300 415 [7].

NOTE 6: This functional grouping is a logical grouping and places no constraints on the physical implementation, e.g. the location of the functionality. Also, it is not constrained to any particular network architecture, e.g. the functionality of a functional group may be distributed across the network, or located at a single place. The relationship between, and the flow of information between functional groupings does not imply the use of any particular protocol.

transit PTNX functionality: This provides functionality to support the relay between originating functionality and terminating functionality. In addition, transit PTNX functionality can provide interconnection with gateway PTNX functionality. Transit PTNX functionality is required when originating functionality and terminating functionality are physically separated. Depending on the routeing of the call, there may be more than one instance of this functionality. (See ETS 300 415 [7]).

NOTE 7: This functional grouping is a logical grouping and place no constraints on the physical implementation, e.g. the location of the functionality. Also, it is not constrained to any particular network architecture, e.g. the functionality of a functional group may be distributed across the network, or located at a single place. The relationship between, and the flow of information between functional groupings does not imply the use of any particular protocol.

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 of 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, 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, comprise 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 PTNXs;
- 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.

NOTE 8: This TCR-TR considers only the case where the shared switched network infrastructures are provided by fixed public networks.

3.2 Abbreviations

For the purposes of this TCR-TR, the following abbreviations apply:

CPE	Customer Premises Equipment
CPN	Customer Premises Network
CN	Corporate telecommunication Network
CTX	CenTralized eXchange
DSS1	Digital subscriber Signalling System No. 1
EC	European Commission
GVNS	Global Virtual Network Services
ISCTX	Integrated Services CenTralized eXchange
ISDN	Integrated Services Digital Network
IVN	InterVening Network

PBX	Private Branch eXchange
PSTN	Public Switched Telephone Network
PTN	Private Telecommunication Network
PTNX	Private Telecommunication Network eXchange
PUM	Personal User Mobility
QSIG	Q interface SIGnalling protocol (ECMA standard)
SIT	Service Information Transport
SRC	Strategic Review Committee
SS7	Signalling System No.7
UPT	Universal Personal Telecommunications
VPN	Virtual Private Network

NOTE: "VPN" is used in conjunction with another term, e.g. "VPN services". The abbreviation is not intended to signify a network itself.

4 General considerations

To date, CNs have been formed by the business community to satisfy their own corporate requirements for telecommunication services. Such networks consist of dedicated equipment, either owned or leased by the organization. The equipment may be geographically dispersed and in general the equipment is connected by means of dedicated connections (e.g. by leased lines), although some proprietary VPN solutions exist.

This TCR-TR examines the requirements for VPNs provided by fixed public networks, whereby all, or some parts of a CN are supported by switched public network infrastructure. The TCR-TR identifies the technical issues to be solved and proposes work items for ETSI TCs.

Within this TCR-TR, VPNs are described in terms of a VPN architecture and VPN services. Corporate customers do not just consider the VPN services, but look upon the VPN architecture as a physical entity which they wish to control and manage. Such customers regard the VPN architecture and the VPN services as a physical part of their CNs.

The VPN architecture is that part of a CN that provides corporate networking between customer equipment using shared switched network infrastructure where:

- the shared switch network infrastructure takes the place of the traditional analogue of digital leased lines and the function of the transit node irrespective of the network type whether it be the 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, 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 public network infrastructure provide:

- VPN end-user services to CN users;
- VPN networking services to support the interconnection of PTNXs;
- service interworking functionality;
- Inter-VPN services to provide co-operation between the VPN services of two networks; and
- VPN management services to enable the service subscribers to control and manage their VPN resources and capabilities.

This TCR-TR consists of two logical parts: clauses 5 and 6 consider the general aspects relating to VPN services; and clauses 7 to 9 consider network aspects relating to the VPN architecture.

4.1 Motivation of work

There are a number of commercial, technical and regulatory pressures which have combined to create an urgent need to identify the impact of standardization activities with regard to VPN.

4.1.1 General market factors

The business community has high demands for sophisticated telecommunication services with networking requirements extending across the globe. The major requirements include:

- facilitation of a competitive market;
- minimal standardization allowing fast implementation;
- world-wide availability;
- independence between services and physical infrastructure;
- removal of arbitrary boundaries between countries;
- encouragement of innovation and new technologies;
- end-to-end management capabilities;
- customisable service offerings;
- lower costs;
- compatibility with already owned equipment; and
- multi-vendor solutions.

All of these requirements indicate a need for greater network harmonization with the removal of barriers to network interconnection.

4.1.2 General technical factors

As corporate networking has developed, a number of technical barriers have emerged which have directed CNs towards the use of certain topologies with service and switching functionality contained only in the end systems (i.e., switching nodes). In particular, services and service interworking for the private and public network domains have developed to some extent independently resulting in some incompatibilities due to the very different requirements which have been placed upon these systems (see TCR-TR 024 [11]). This aspect, together with certain regulatory restrictions, has tended to limit the public network involvement in corporate networking to the provision of transparent interconnection of PBXs via leased lines.

It is essential, if the market requirements are to be met, to work towards removing technical incompatibilities to enable networks to co-operate fully in supporting the functionality required for corporate networking. This means that eventually a full harmonization of services in the private and public network domain should be sought. Not just the replacement of leased lines with a switched public network capability. The commercial and service requirements will require the location of functionality to be flexibly determined on both technical and cost grounds.

4.1.3 General regulatory factors

The third phase of community policy was initiated by the 1993 services review which included two points of major relevance for standardization in the area of corporate networks.

a) The review concluded that standardization activities should concentrate on network access, network interconnection, interoperability and trans-European networks. Such standards will greatly facilitate the support of corporate networking with functionality distributed over a number of co-operating networks.

b) It is intended that full liberalization of all public voice telephony services will be achieved by 1998 subject to additional transitional periods for less developed and very small networks. This liberalization will effectively abolish the traditional distinction between private networks and public networks thus fundamentally changing the conception that corporate networks are synonymous with networks provided wholly by privately owned equipment. The liberalized environment will mean that corporate networks will be able to utilize the capabilities of all networks working together in co-operation to support the services required by the end users. The end users of the corporate network will not only be connected to traditional PBXs but also directly to traditional public network local exchanges.

4.2 VPN motivations

Corporate customers expect VPN services to be more cost effective and to provide more flexible CN solutions than those obtainable by leased lines for linking of geographically dispersed corporate CPE. At the same time it is expected that the VPN services will contribute to the increased productivity between the geographically dispersed corporate employees.

For the Telecom Operator, VPN services means a cost optimized utilization of the public network infrastructure by replacing leased lines by a **switched** public network infrastructure based service. At the same time it opens up a possibility to provide added values such as call routeing, Centrex based services out-sourcing and network management agreements.

5 Service aspects - conceptual framework

5.1 VPN services in context of CN

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.

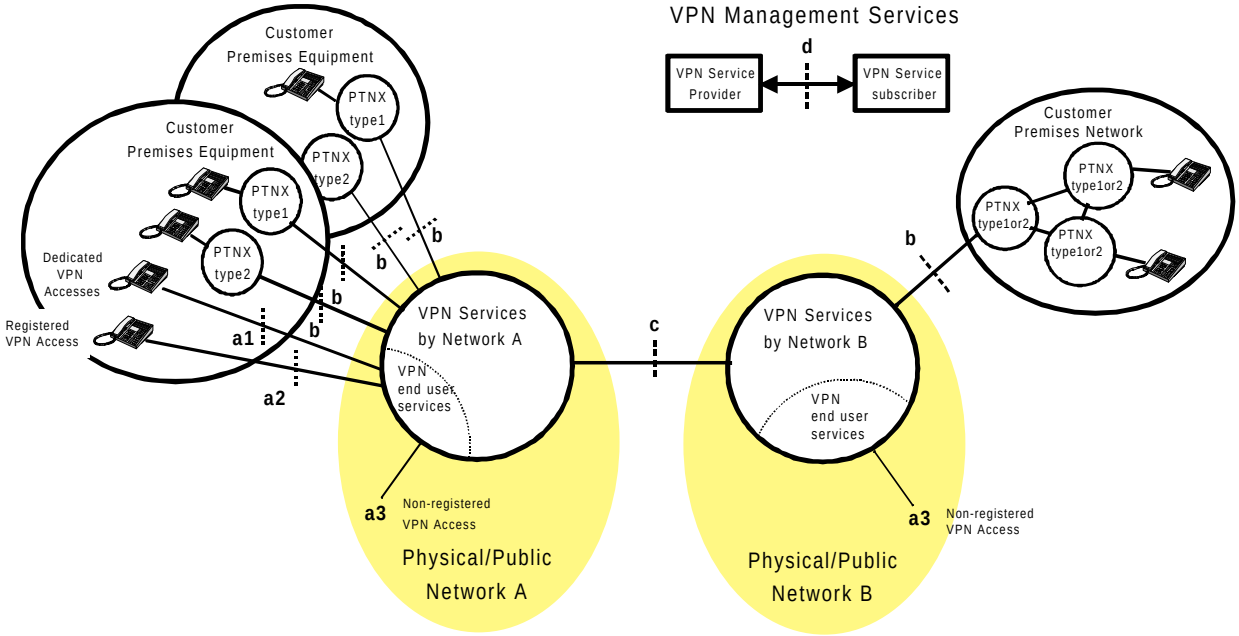
The following PTNX types are defined:

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

PTNX type 2: An implementation of a PTNX outside the public network that supports services based on PTN standards (see annex B) in addition to the services provided by the public ISDN and/or PSTN.

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

a) VPN end-user services: services offered at the a1, a2 and a3 service entry points;
b) VPN networking services: services offered at the b service entry point;
c) Inter-VPN services: services offered at the c service entry point;
d) 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 their 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"[2)] . By means of an appropriate authentication procedure a pre-defined set of VPN end-user services become available to the CN user.

b: The b service entry point for PTNX type 2 and PTNX type 1. At this service entry point VPN networking services are provided to PTNX type 2 and PTNX type 1 for the provision/support of services to its end-users.

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.

---

2) This is also known as "remote CTN access".

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.

6 Service aspects - service requirements

VPN services can be considered as a set of services and functionalities which may be tailored to the specific needs of each corporate customer. A minimum set of service features are expected to be commonly present in all VPN service offerings, being referred to as "core" VPN service features. Other service features may not always be available or may be offered on an optional basis.

Core features of VPN services include:

- private numbering plan which allows a CN user to address a called party by a private number, i.e. a number which is assigned by the CN administrator independently of the public network access on which the relevant CPE is attached;

- the support of internal CN calls made via a1, a2, a3, and b service entry points;

- the support for a calling user in the CN to originate calls to users outside the CN (e.g. public network subscribers addressed by a public number, public network subscribers addressed by a specific CN number, or users in another CN that can be called from outside their CN);

- the support for a called user in the CN to receive calls from a user outside the CN; and

- remote access procedures to allow secure access at the a3 service entry point.

Some examples of optional VPN service features are:

- abbreviated dialling and speed dialling enabling a CN end user to dial short numbers which are either pre-registered for the whole CN or registered by a specific access for its own use; and

- call screening enabling the CN administrator to define the rights attached to a CN user or access. Such rights can be used to define the group of CN users who can call a specific user, to make restrictions on the outgoing calls of a specific CN end user (e.g. forbid public numbers) or the incoming calls to a specific access (e.g. forbid all the incoming calls from the public network).

6.1 VPN end-user services

6.1.1 The a1 service entry point (dedicated VPN access)

At the a1 service entry point, VPN services include the ability to make private calls within a predetermined CN as well as calls external to the CN. At the a1 service entry point, a pre-defined set of specific VPN end-user services is permanently available to the CN user.

6.1.2 The a2 service entry point (registered VPN access)

At the a2 service entry point, the CN user is provided with two modes of operation, the CN mode and the public network mode. A specific mechanism allows the user to swap between the two modes.

In the CN mode, VPN services include the ability to make private calls within a pre-determined CN as well as calls external to the CN. There is no need for a complete identification and authentication procedure to be able to use VPN services at the a2 service entry point (an automatic calling line identity screening procedure can be used). In the CN mode, the services offered at the a2 service entry point in principle should be the same as those offered at the a1 service entry point (depending on the specific implementation and/or capabilities in the public network(s)).

NOTE: In principle, some networks may allow registration for more than one CN.

When the public network mode is selected, all the functionalities of a public network access are available at the a2 service entry point.

6.1.3 The a3 service entry point (non-registered VPN access)

At the a3 service entry point, a remote access procedure is required to allow the user to gain access to a CN from a public network access which is not registered as an access to that CN. This allows the user (or terminal on behalf of user) to:

- indicate to the public network that access to the CN is requested (e.g. through a special dialling prefix in the called number);
- identify and authenticate oneself as a participating CN user (e.g. through some password procedures similar to those of a card calling service).

The remote access procedure for the a3 service entry point may be provided through service procedures which do not necessarily impose additional requirements on the protocol of the user-network interface. As soon as the end user has successfully completed the remote access procedure he/she is considered to be participant of the CN for that particular call instance and is allowed to utilize the relevant VPN end-user services. Optionally, a registration procedure may allow the user to receive CN calls (e.g. for a limited period).

The remote access procedure allows CN users which are "travelling around" to, in principle, access the VPN services from any geographical location (for example to have the call billed on the account of the corporation). This is consistent/similar with principles laid down in the Universal Personal Telecommunications (UPT) concept as studied in ITU-T (SG1) and ETSI (STCs NA1/NA7) and Personal User Mobility (PUM) in STC BTC1.

After successful completion of a remote access procedure, the a3 service entry point, in principle, supports the same services as on the a1 service entry point. The provision of services at the a3 service entry point is dependent on the specific implementation and/or capabilities in the public network(s). The result may be that only a subset of the services can be made available to that CN user.

6.1.4 Work items relating to the a service entry point

The differences between the a1, a2, and a3 services entry points may be summarized as follows:

Table 1: Comparison of the a1, a2 and a3 services entry points

	a1	**a2**	**a3**
Characteristics	dedicated	registered	non-registered
user procedures to access VPN services	none required	procedure required to swap between CN mode and public network mode	procedure required
authentication	not required	see note	required
VPN services available	always	only in CN mode	only after access procedure
NOTE: The requirement for authentication should be considered as part of work item 3.			

The following work items result from the discussions in subclauses 6.1.1 to 6.1.3.

Work item 1:	Study of VPN end-user service requirements at the a1, a2 and a3 service entry points and the production of relevant service descriptions.
Responsible TC:	NA
Interested TCs/STCs:	SPS, BTC1, ECMA TC32 TG13
Description:	TC NA and ECMA TC32 have developed a number of service descriptions for both basic and supplementary services for implementation in public networks and private networks (see annex A and annex B). In addition, Global Virtual Network Services (GVNS) service requirements are being studied in ITU-T SG1 (see annex C). TC NA should study which of the requirements within these service descriptions are subject to standardization in context of the a1, a2 and a3 service entry points. Service interworking between pairs of these service entry points, and between these service entry points and other service entry points should be considered. Stage 1 service descriptions are to be produced with the aim of providing input to other studies (e.g. protocol studies in SPS or IN studies in NA). Where appropriate NA should consider adopting or enhancing existing ETSs.

Work item 2:	Study of remote access service requirements at the a3 service entry point and the production of relevant service descriptions.
Responsible TC:	NA
Interested TCs/STCs:	SPS, BTC1, ECMA TC32 TG13
Description:	TC NA should study the requirements of the remote access service procedures to allow gaining access to the CN at the a3 service entry point. NA should investigate appropriate authorization and security aspects. Stage 1 service descriptions are to be produced with the aim to provide input to other studies (e.g. protocol studies in SPS).

Work item 3:	Study of the requirements for changing between CN mode and public network mode (and vice versa) at the a2 service entry point and the production of relevant service descriptions.
Responsible TC:	NA
Interested TCs/STCs:	SPS, BTC1, ECMA TC32 TG13
Description:	TC NA should study the requirements of the procedures to allow gaining access to the CN at the a2 service entry point. NA should investigate appropriate authorization and security aspects. Stage 1 service descriptions are to be produced with the aim to provide input to other studies (e.g. protocol studies in SPS).

6.2 VPN networking services

6.2.1 The b service entry point

The PTNX type 1 and PTNX type 2 at the b service entry point requires service interoperability that goes beyond those defined for the common use within the public network (PSTN/ISDN). The services offered at this service entry point are in principle a combination of:

- support of public supplementary services;
- support of private network services;
- support of Service Information Transport (SIT);
- support of additional services based on intelligent network implementations.

NOTE: This list is an attempt to identify an extensive set of service requirements regarding the b service entry point, and is not meant to be a list of mandatory requirements.

Work item 4:	Study of VPN networking service requirements at the b service entry point.
Responsible TC:	NA
Interested TCs/STCs:	SPS, BTC1, ECMA TC32 TG13
Description:	NA should study VPN networking services required at the b service entry point. These services could include: - support of public supplementary services; - support of private network services; - support of SIT; - support of additional services based on intelligent network implementations. Service interworking between the b service entry point and other service entry points should be considered. In addition service interworking between PTNX type 2 and PTNX type 1 needs to be considered. If the BTC1 studies on the integrated scenario are found to be relevant to this work item, BTC1 should provide NA with its expertise.
NOTE 1:	Studies of SIT should consider the need for network protection mechanisms (e.g., service screening, congestion control etc.).
NOTE 2:	Some PBXs will only use a subset of the VPN networking services.
NOTE 3:	All bullet items have equal priority.

6.2.2 Inter-VPN services

It is recognized that VPN services can span multiple public networks and be based on different VPN service provisions in each of the involved public networks. The provision of such an "international VPN service" will have to rely on functionalities which will be located in separate public networks. The way the functionalities involved in this international VPN service provision needs to be studied in order to define the signalling requirements at the international interface. For example, the case of queries to remote databases should be investigated in order to allow VPN services offered by different service providers to exchange data concerning a particular CN.

Work item 5:	Study of the functional requirements at the c service entry point.
Responsible TC:	NA
Interested TCs/STCs:	SPS, BTC1, ECMA TC32 TG13
Description:	NA should investigate the co-operation between functionalities located in different public networks for the provision of an "international VPN service". In particular, the exchange of information for the support of calls and services between the different VPN service providers needs to be investigated. The resulting requirements should be given to SPS as a basis for the development of protocols. In the case of an IN implementation, NA6 should investigate the information model used to support the VPN services. In addition, NA6 should consider interworking between IN based and non-IN based networks. Service interworking between the c service entry point and other service entry points should be considered.

6.3 VPN management services

Below, a set of VPN management services has been identified. This set is not meant to be exhaustive but just to give an overview of the VPN management areas and a brief description of these items is given in annex E:

- single point of contact;
- VPN data management;
- performance management;
- fault management;
- security management;
- customer control procedures;
- supervisory management service;
- management of CN numbering plans;
- routeing administration;
- customized recorded announcements;
- call logging;
- statistical information;
- flexible billing.

NOTE: No detailed requirements for the listed VPN management services have been identified yet. An organizational model for pan-European VPN services showing the management relationships between the VPN service providers, VPN service subscribers, and possibly other organizational entities is for further study.

Work item 6:	Study of VPN service management requirements at the d service entry point and the production of relevant service descriptions.
Responsible TC:	NA
Interested TCs/STCs:	BTC1, ECMA TC32 TG12
Description:	NA should study the requirements at the d service entry point. This includes the definition of an organizational model for pan-European VPN services that shows the management relationships between the VPN service providers, VPN service subscribers, and possibly other organizational entities. Functional descriptions are to be produced with the aim of providing input to other studies concerning architecture, protocols, modelling, etc..

7 Networking aspects - CN network models

This clause provides 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 8.

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).

Possible implementation scenarios for a CN are illustrated in annex D based upon different solutions for VPN service offering.

7.1 Relation between service entry points and reference points

Figure 2 shows the relation between service entry points as described in clause 5 and reference points defined in the reference configurations applying for private and public ISDNs. The entry points are surrounded by quotation marks (e.g. "a1") so as not to confuse them with reference points.

The "VPN service" in figure 2 is represented by the following functional groupings:

- transit PTNX functionality;
- end PTNX functionality;
- gateway PTNX functionality;
- public VPN services.

The term "end PTNX functionality" is defined in ETS 300 415 [7].

The term "public VPN service" represents the group of functions that can be provided by the public network based on services defined for the public ISDN, but with enhancements to support CN functions.

The b service entry point to VPN services can apply either at the T reference point or the Q reference point:

- the T reference point applies for PTNX type 1. VPN services that are provided at the b service entry point are supported by means of the "public VPN service";
- the Q reference point applies for PTNX type 2. VPN services that are provided at the b service entry point are supported by means of transit PTNX functions.

The a1 service entry point to VPN services can apply either at the S reference point or the S/T reference point:

- VPN services provided by the "end PTNX functionality" applies at the S reference point;
- VPN services provided by the "public VPN service" applies at the S/T reference point.

The a1 service entry point is dedicated to VPN services and an escape mechanism is required to obtain access to the public network.

The a2 service entry point applies at the S/T reference point. A user can obtain access to either the "public VPN service" or the public ISDN service via the a2 service entry point.

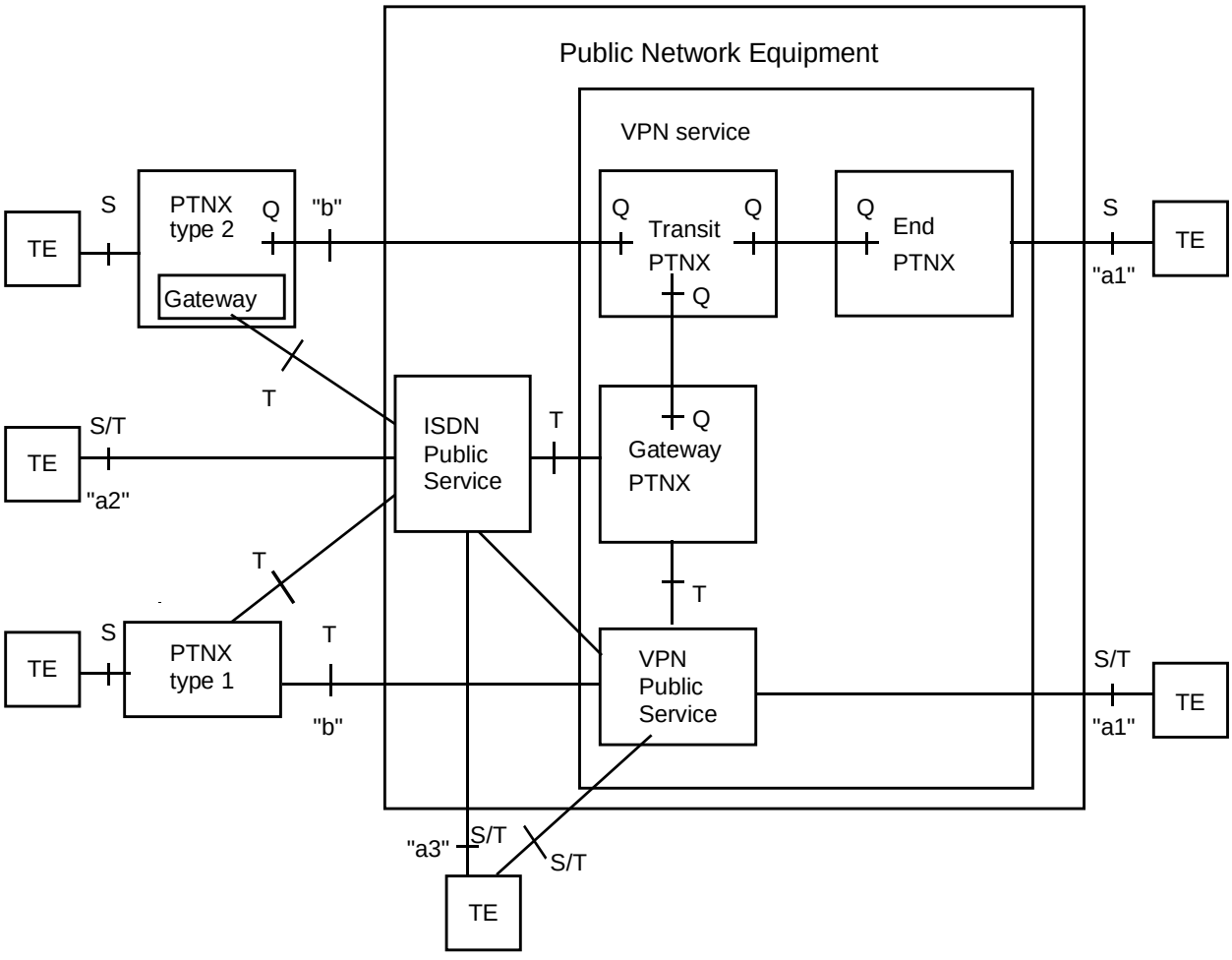
The a3 service entry point applies at the S/T reference point between a TE and the public ISDN. A non-registered access procedure is needed to obtain access to VPN services. This is explained more in detail in subclause 7.2.3.

Interconnection between PTNX type 1 and PTNX type 2 requires an interworking function for those CN services that operate differently over the T reference point and over the Q reference points. This implies that the functionality for services that are used between users at PTNX type 1 and PTNX type 2 may be reduced. This interworking function is performed by the gateway PTNX functionality that is part of VPN services.

Similarly, an interworking function may be needed for services used between the a1 service entry point to the "public VPN service", and the a1 service entry point to the "end PTNX functionality".

The PTNX type 2 obtains access to the public ISDN service via a gateway PTNX functionality. This functionality may be either located in the PTNX type 2 or be part of VPN services.

The gateway PTNX functionality which is part of VPN services provides access to the public ISDN services and is required in the model in order to support the operation of services that may result in a call intended to be within the CN but is routed to a user outside the CN (for example, the called user in the CN has activated forwarding to a user outside the CN). Whilst the gateway PTNX functionality is required for the model, it need only be available in networks which support this functionality.



NOTE: The interconnection of the PTNXs to the public network equipment may be provided by a new reference point called T+ (see TCR-TR 033 [13] for further details).

Figure 2: Relation between service entry points and reference points for ISDN services

Different interface and gateway arrangements may exist for PTNX type 2:

a) The PTNX has separate interfaces to "VPN services" and "public ISDN services". In this case either the gateway PTNX functionality in the PTNX type 2 or the gateway functionality that is part of "VPN services" is used depending on the service used and the call case.

b) The PTNX has only access to "VPN services". In this case, the gateway functionality in "VPN services" is mandatory, if access to the public ISDN service is required. In this case public ISDN services need to be made available at the Q reference point.

c) The PTNX has a shared interface to access "VPN services" and public ISDN services. In this case a mechanism is required to separate whether "VPN services" or public ISDN services shall be used. The gateway functionality that is part of "VPN services" is in this case, not mandatory. Both the Q and the T reference point will in this case apply at the same interface.

Call cases between the different terminals are described more in detail in the following subclauses.

7.2 PTNX type 2, 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 PTNX", "terminating PTNX", "transit PTNX", and "gateway PTNX" functions.

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

7.2.1 Connections between PTNXs

Figures 3 and 4 show 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 PTNX and transit PTNX). In such cases, an interface at the C reference point will exist.

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

In figures 3 and 4, the IVN functional grouping is only shown between the originating PTNX functionality and the transit PTNX functionality, and also between the transit PTNX functionality and the terminating PTNX functionality. By definition, the transit PTNX functionality will be physically separated from the originating PTNX functionality and also the terminating PTNX functionality. In other cases functional groupings, e.g. the transit PTNX functional grouping and the incoming gateway PTNX 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.

7.2.2 Structured overview of the functional groupings which may be involved in a call

Figure 3 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 may be null. In addition, a PTNX implementation

will contain a number of the functional groupings in the figure, although the functional groupings will not all be used on a call.

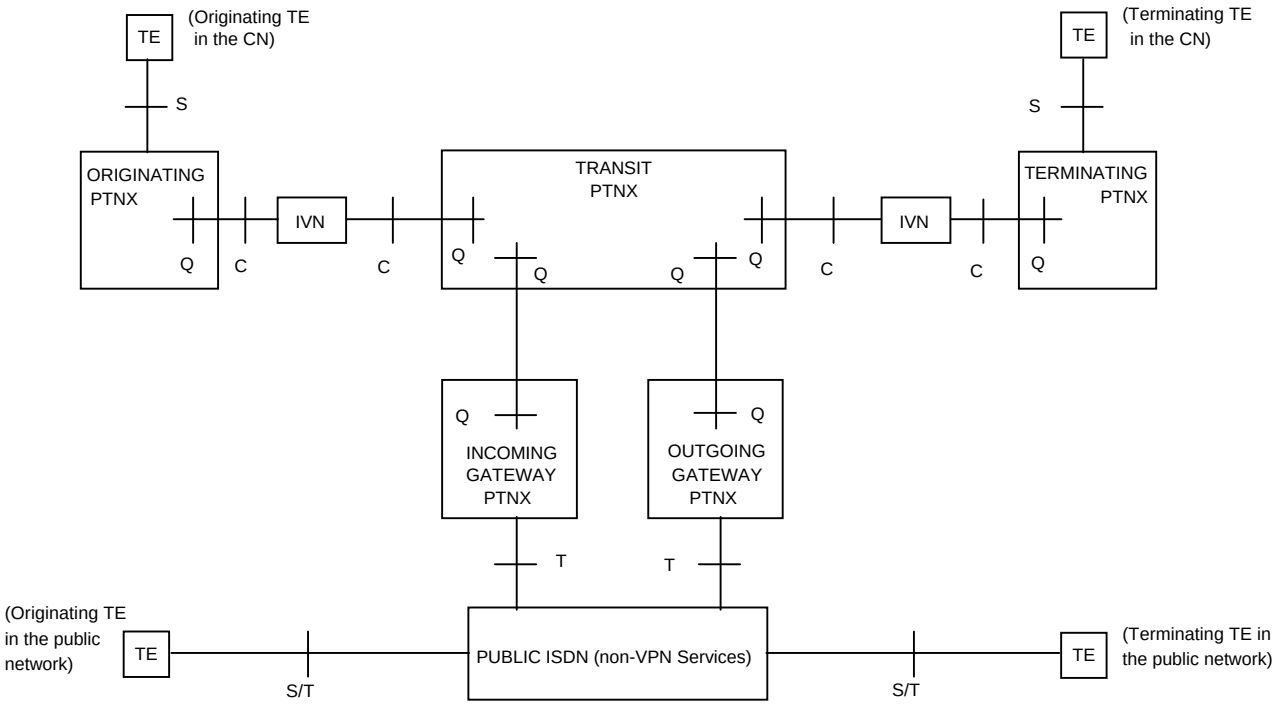


Figure 3: PTNX type 2, structured overview of the functional groupings that may be involved in a CN call

"Public ISDN" shown in figure 3 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 3 should be read from the left (originating functionality) to the right (terminating functionality) for call examples as follows:

a) 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 PTNX, through the CN via transit PTNX(s) to the terminating PTNX, and then to the "terminating TE in the CN";

b) 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 PTNX, passes through the CN via transit PTNX(s) to the terminating PTNX, and then to the "terminating TE in the CN";

c) 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 PTNX, through the CN via transit PTNX(s) to the gateway PTNX, 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 PTNX functionality on a call (i.e. four or more PTNXs are involved in the call) and if the communication link between two of the transit PTNXs is congested or out of service, alternative routeing mechanisms could route the call via the public network.

Figures 5 to 9 are based on figure 3 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.

7.2.3 Structured overview including non-registered CN access

Non-registered CN access enables users whose equipment is attached to the public network, but is not registered as having access to the CN, to identify themselves to the CN and be given access to CN services. Services available to users gaining access to the CN in this manner correspond to VPN services applicable to a3 service entry point.

Security mechanisms need to be employed in order to prevent unauthorized access. An example of the use of non-registered CN access is where the user has a full service profile registered with the CN, but is temporarily located elsewhere. On gaining access to the CN, some or all of the user's services are made available to the user at the temporary location.

Figure 4 is based on figure 3 and includes functional groupings and relationships between them which are required to support non-registered CN access. The additional functional groupings are:

- "non-registered CN access authorization" that provides functionality to support the security mechanisms used by the CN (e.g. prompting the user for a password, checking the validity of the password provided);

- "non-registered CN access originating agent" that provides functionality to support the non-registered user as a user in the CN (e.g. calls originated by the non-registered user will be seen as calls originated by a user attached to the CN); and

- "non-registered CN access terminating agent" that provides functionality to support the non-registered user as a called user in the CN.

NOTE: The need for the remote CN access terminating agent will depend on the details of the service description.

The relationships r_w, r_x, r_y, and r_z are used to indicate that there are information flows between functional groupings.

Subclauses 7.2.3.1 and 7.2.3.2 describe the functionality relating to non-registered users making and receiving calls within their CN.

7.2.3.1 Use of a non-registered access by an originating user in a CN

With regard to the relationships between the functional groupings identified in subclause 7.2.3 and other functional groupings in figure 4, there are three stages in the process of a non-registered user gaining access to the CN as a CN user. Depending on the actual implementation, this process may be a single step whereby all of the information is provided by the user in a single request, or the process may consist of a number of steps performed sequentially.

These three stages are described sequentially, and at each stage only some of the functional groupings and the relationships between them are involved. The three stages operate as follows:

Stage 1

The user generates a call from a terminal connected to the public network and indicates that access to the CN is required. Where there is no association between the user and the required CN, the user will need to identify the CN explicitly.

As for item b) in subclause 7.2.3, 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 incoming gateway PTNX functionality which supports the remote access mechanism.

During this process, the various functional groupings interact as normal, and no functionality is performed by the additional functional groupings identified in this subclause.

Stage 2

The incoming gateway PTNX then evaluates the calling user's request for access as a CN user.

At this point, functionality in the CN performs the "non-registered CN access authorization" which may entail the recognition of passwords or the support of other security measures. The actual mechanisms employed are outside the scope of this TCR-TR.

This functionality overlays the existing call and relationship r_x exists between the originating TE in the public network and the non-registered CN access functional grouping, and also relationship r_y exists between the non-registered CN access functional grouping and the incoming gateway PTNX functional grouping. Once the authorization procedures are completed, resulting in either acceptance or rejection, this overlaid functionality will cease to operate.

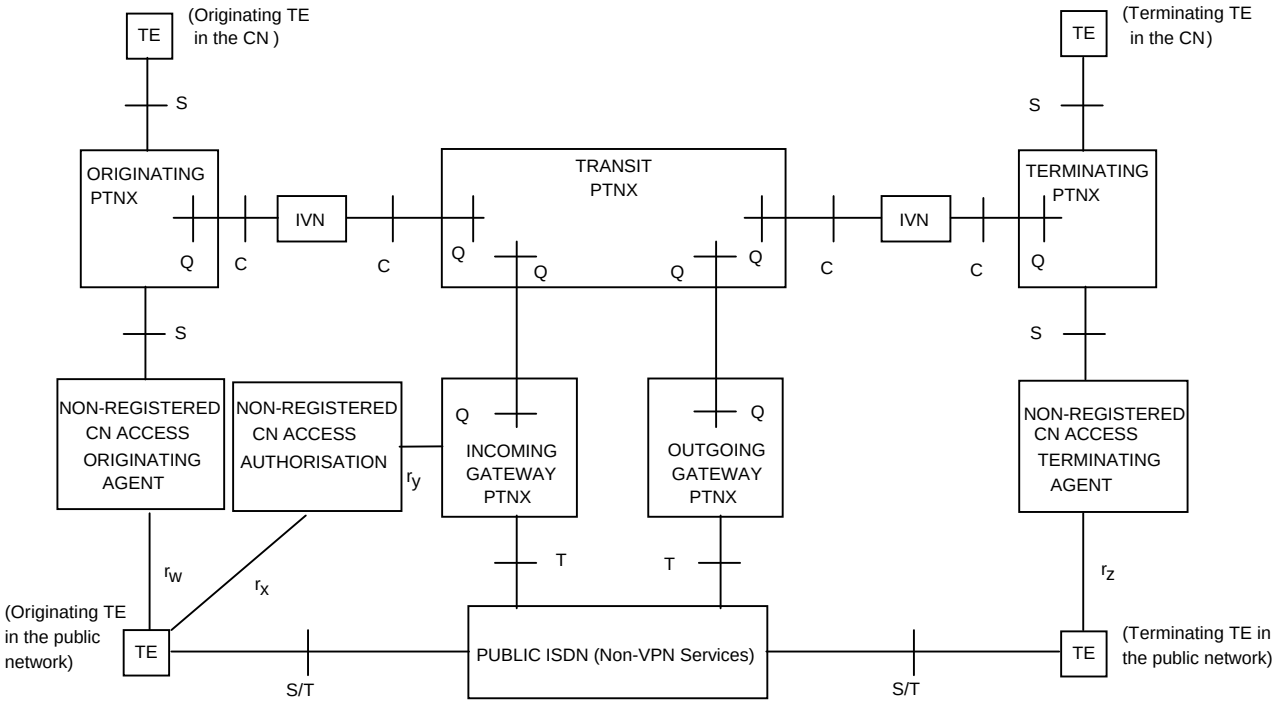


Figure 4: PTNX type 2, structured overview that includes CN access

Stage 3

After the user is granted access, the user in the public network is then considered as a user connected to the CN and can use the services of the CN. This use may be restricted e.g., due to security considerations, or the capabilities of the terminal or networks involved.

After the user has been granted access, the non-registered CN access originating agent functional grouping is employed to provide the bridge between the originating TE in the public network and the entity in the CN where the user logically resides.

This functionality overlays the existing call and the relationship r_W exists between the originating TE in the public network and the non-registered CN access originating agent functional grouping.

In addition, the non-registered CN access originating agent is seen by the originating PTNX to be logically connected via the S reference point.

NOTE: There is an instance of a basic call between the originating TE in the public network and the incoming gateway for the purposes of gaining access to the CN, and after this access is successful, there is an instance of a basic call between this TE functionality (now considered as the originating TE in the CN) and the destination user in the CN. Depending on the implementation of the remote access mechanism, these may merge into a single instance of a basic call, but in other implementations, e.g. where a PTNX performs the functionality instead of the VPN service, the two instances of the basic call can coexist and the instance of the basic call in the CN will overlay the instance of the basic call in the public network.

7.2.3.2 Non-registered user as a terminating user in a CN

Functionality similar to that in stage 3 in subclause 7.2.3.1 needs to exist in the case where the destination of a call in the CN is logically a terminating TE in the CN, but actually resides in the public network. This implies that there is an association between the user considered as a member of the CN and the user's actual location.

In this case, the call is routed through the CN to the terminating PTNX functional grouping where the user logically resides, and this results in a normal call into the public network via the outgoing gateway PTNX to the terminating TE in the public network.

The non-registered CN access terminating agent functional grouping is employed to provide the bridge between the entity in the CN where the user logically resides and the terminating TE in the public network. This functionality overlays the call and the relationship r_Z exists between the non-registered CN access terminating agent functional grouping and the terminating TE in the public network.

In addition, the non-registered CN access terminating agent is seen by the terminating PTNX to be logically connected via the S reference point.

NOTE: There is an instance of a basic call between originating user in the CN (which may have accessed the CN as described in subclause 7.2.3.1) and the terminating TE in the CN (where that user logically resides) and there is an instance of a basic call between the outgoing gateway and the terminating TE in the public network for the purposes of routeing the call to the actual destination. Depending on the implementation of the remote access mechanism, these may merge into a single instance of a basic call, but in other implementations, e.g. where a PTNX performs the functionality instead of the VPN service, the two instances of the basic call can coexist and the instance of the basic call in the CN will overlay the instance of the basic call in the public network.

7.2.4 Transit networking service provided by the public network

Figure 5 contains an example where the transit and gateway functional groupings for calls are provided by the public network. Services provided to the PTNX containing the originating PTNX functionality and also to the PTNX containing the terminating PTNX 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 PTNX functionality and the transit PTNX functionality, and also between the transit PTNX functionality and the terminating PTNX functionality shown in figure 3 is considered to reside in the public network and, as a result this functionality is not shown in figure 5.

The IVN functionality which resides in the public network is outside the scope of this TCR-TR.

The support of non-registered CN access shown in figure 4 is not shown in figure 5. However, the non-registered CN access authorization functional grouping could also be provided by the public network.

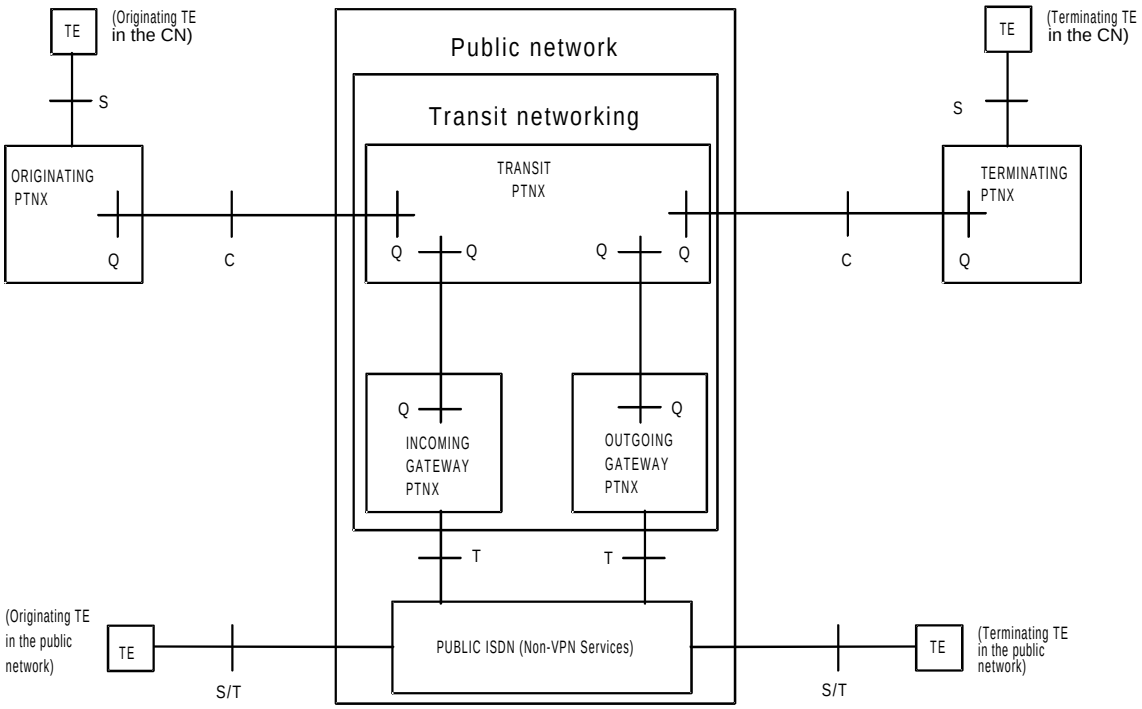


Figure 5: Transit networking service provided by the public network

7.2.5 Transit and terminating functions provided by the public network

Figure 6 contains an example where the terminating functional grouping is also provided by the public network. Services provided to the PTNX containing the originating PTNX 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 PTNX and the terminating PTNX functional groupings resides in the public network. Also, the IVN functionality between the originating PTNX functionality and the transit PTNX functionality shown in figure 3 is considered to reside in the public network and, as a result this functionality is not shown in figure 6.

All of the IVN functionality which resides in the public network is outside the scope of this TCR-TR.

In practice, the public network would also provide an originating PTNX functional group (see figure 7), but the purpose of the example in figure 6 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 PTNX functional grouping is provided by the public network and the terminating PTNX 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 PTNX containing the terminating PTNX functionality correspond to VPN services applicable to the b service entry point.

Similar to figure 5, figure 6 does not show the support of non-registered CN access. In the case of this example, the non-registered CN access authorization functional grouping could be provided. Also the non-registered CN access terminating agent functional grouping could be provided by the public network.

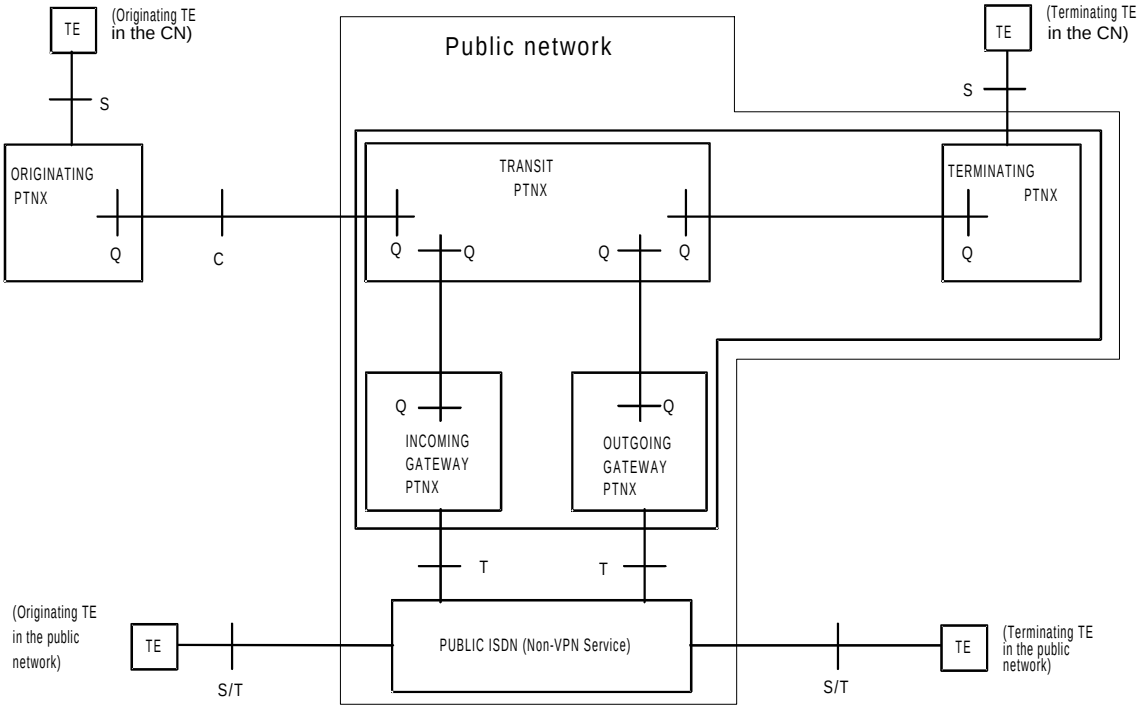


Figure 6: Transit and terminating functional provided by the public network

7.2.6 Transit, originating and terminating functions provided by the public network

Figure 7 contains an example where the originating, transit and terminating functional grouping is provided by the public network. Services provided to the user at the originating end of the call and services provided to the user at the terminating end of the call correspond to VPN services applicable to the a1 service entry point and 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 PTNX and the terminating PTNX functional groupings resides in the public network. Also, the IVN functionality between the originating PTNX functionality and the transit PTNX functionality shown in figure 3 is considered to reside in the public network and, as a result this functionality is not shown in figure 7.

All of the IVN functionality which resides in the public network is outside the scope of this TCR-TR.

Similar to figure 5, figure 7 does not show the support of non-registered CN access. In the case of this example, the non-registered CN access authorization functional grouping could be provided. Also the non-registered CN access terminating agent functional grouping could be provided by the public network.

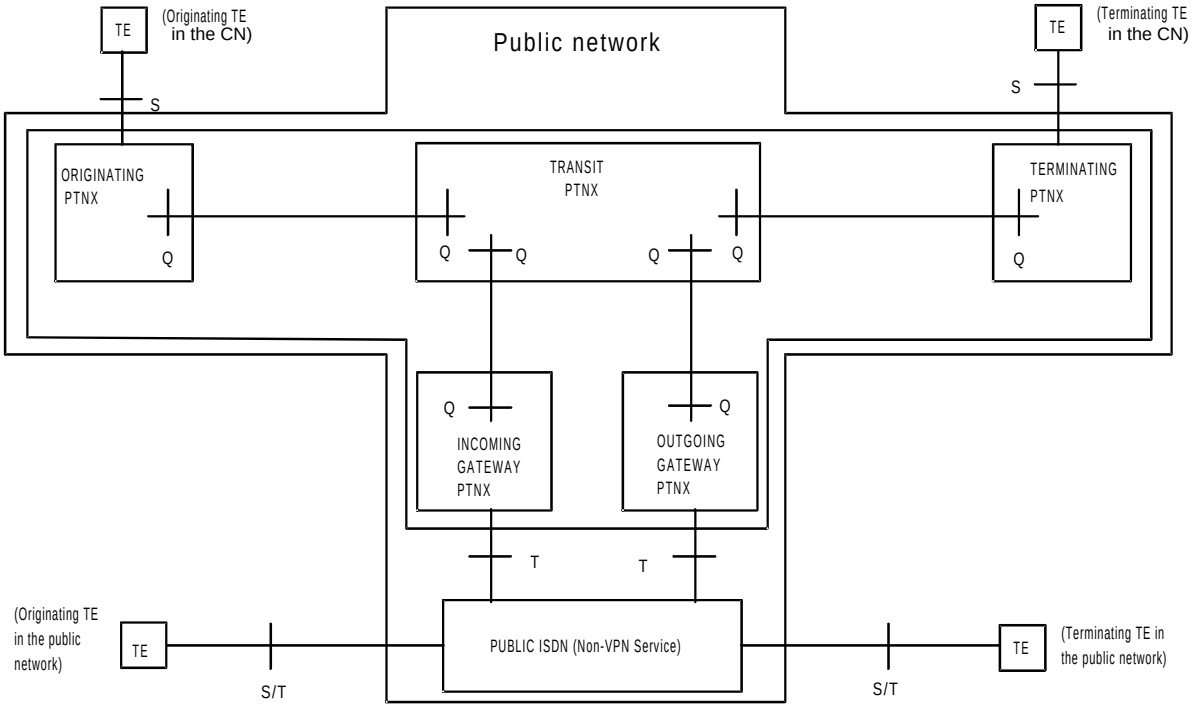


Figure 7: Transit, originating and terminating functions provided by the public network

7.2.7 Involvement of two public networks, with one providing transit networking only

Figure 8 contains an example where two public networks are involved, one providing only transit functionality, and the other also providing the terminating functional grouping. Services provided to the PTNX containing the originating PTNX functionality correspond to VPN services of public network 1 which are applicable to the b service entry point. Services provided to the user at the terminating end of the call correspond to VPN services of public network 2 which are applicable to the a1 service entry point and the a2 service entry point.

The individual functional groupings are shown separately within each of the public networks, but, other than constraining the separation of the two public networks, this is not intended to make any recommendations to constrain the implementation.

In this example, the IVN functionality between the transit PTNX and the terminating PTNX functional groupings resides in public network 2. Also, the IVN functionality between the originating PTNX functionality and the transit PTNX functionality shown in figure 3 is considered to reside in public network 1 and, as a result this functionality is not shown in figure 8.

All of the IVN functionality which resides in the public network is outside the scope of this TCR-TR.

In figure 8, the reference point between the transit PTNX functional grouping has been marked "N*" for the time being. The properties of this reference point need to be defined. Further investigation is needed. Depending on the implementation, the protocols at the N* reference point and at the N reference point may be similar.

In practice, public network 2 would also provide an originating PTNX functional group (see figure 9), but the purpose of the example in figure 8 is to model calls where the caller is connected to a physical PBX, or public network 1.

Also, an additional figure could be drawn in order to model calls where the originating PTNX functional grouping is provided by public network 1 and the terminating PTNX 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 of public network 1 which are applicable to the a1 service entry point and services provided to the PTNX containing the terminating PTNX functionality correspond to VPN services of public network 2 which are applicable to the b service entry point.

Similar to figure 5, figure 8 does not show the support of non-registered CN access but that could also be provided.

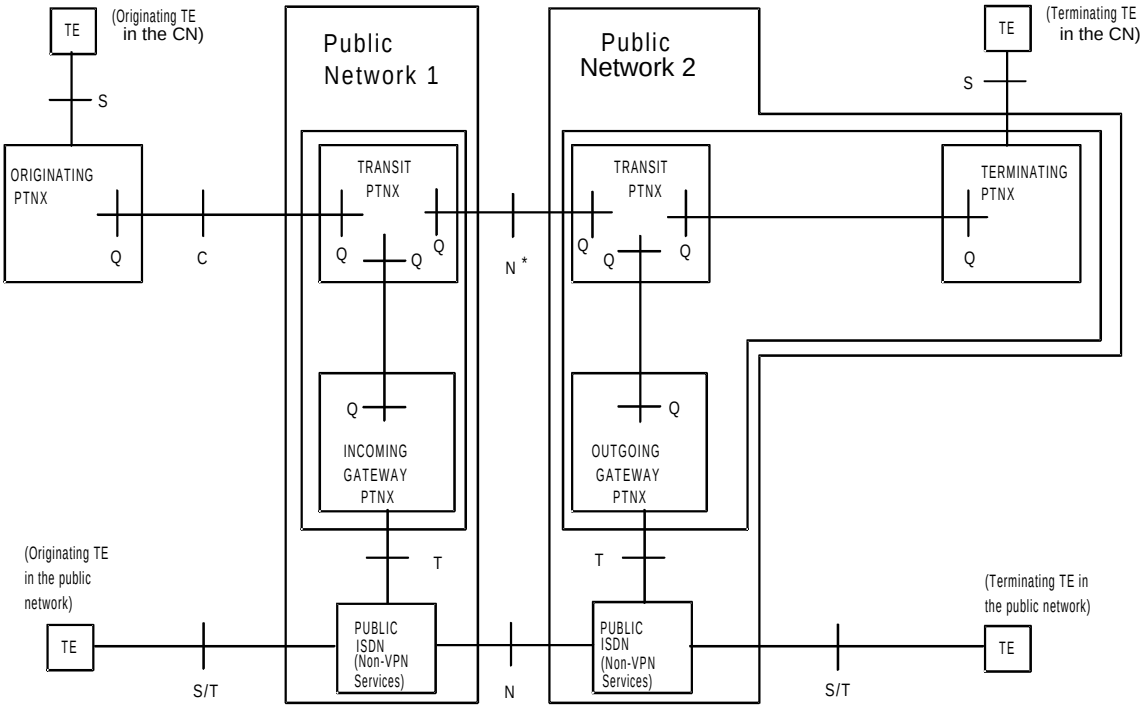


Figure 8: Functional groupings distributed between two public networks

7.2.8 Involvement of two public networks providing originating and terminating functionality

Figure 9 contains an example where two public networks are involved, one providing the originating functional grouping and transit functionality, and the other providing transit functionality and the terminating functional grouping. Services provided to the originating user correspond to VPN services of public network 1 which are applicable to the a1 service entry point and at the a2 service entry point. Services provided to the user at the terminating end of the call correspond to VPN services of public network 2 which are applicable to the a1 service entry point and at the a2 service entry point.

The individual functional groupings are shown separately within each of the public networks, but, other than constraining the separation of the two public networks, this is not intended to make any recommendations to constrain the implementation.

In this example, the IVN functionality between the transit PTNX and the terminating PTNX functional groupings resides in public network 2. Also, the IVN functionality between the originating PTNX functionality and the transit PTNX functionality shown in figure 3 is considered to reside in public network 1 and, as a result this functionality is not shown in figure 9.

All of the IVN functionality which resides in the public network is outside the scope of this TCR-TR.

As in figure 8, for the time being, the reference point between the transit PTNX functional grouping has been marked "N*" in figure 9. The properties of this reference point need to be defined. Further investigation is needed. Depending on the implementation the protocols at the N* reference point and at the N reference point may be similar.

Similar to figure 5, figure 9 does not show the support of non-registered CN access but that could also be provided.

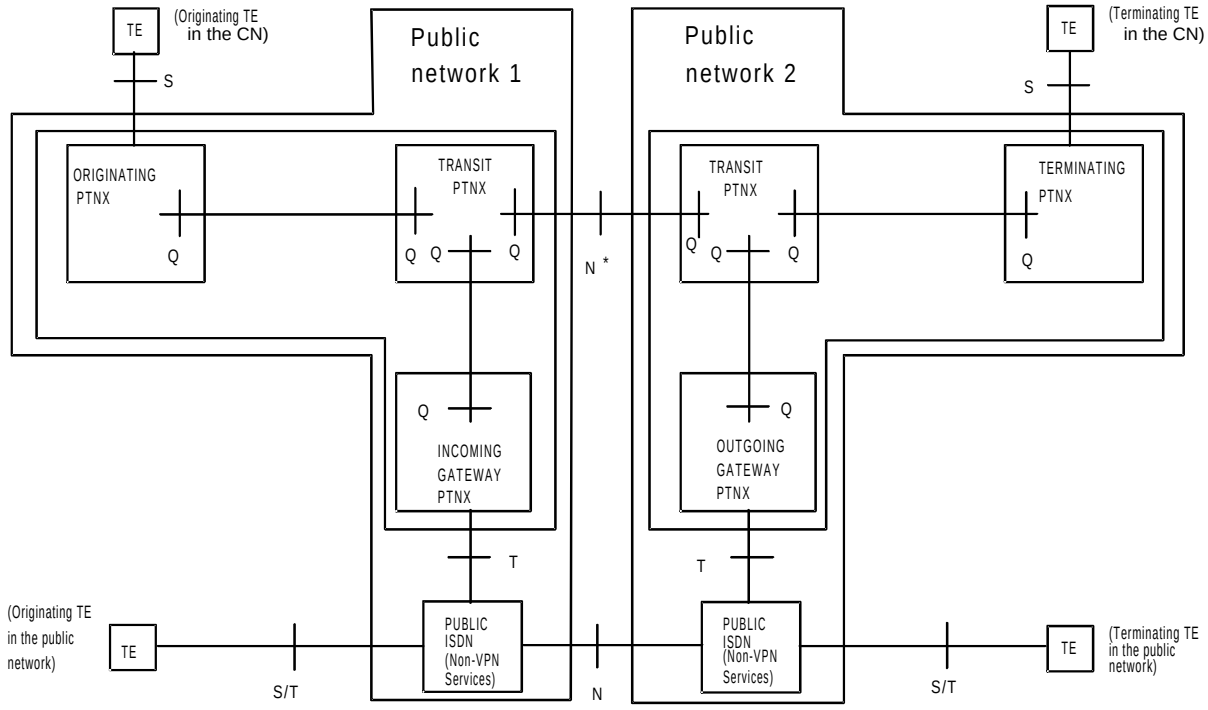


Figure 9: Functional groupings distributed between two public networks

These functional groupings are logical groupings and place no constraints on the physical implementation, e.g. the location of the functionality. Also, functional groupings are not constrained to any particular network architecture, e.g. the functionality of a functional group may be distributed across the network, or located at a single place.

In the figures and their explanations below references to "originating PTNX" should be understood as meaning "the implementation of the originating PTNX functional grouping". This does not necessarily mean implementation in one (or more) physical PTNX(s).

7.3 Functional model of a CN including the public VPN service

Figure 10 shows functional groupings that may be involved in calls to and from users whose terminals are attached to PTNX type 1. Figure 10 shows the functional grouping "public VPN service" included in a CN. This functional groupings supports PTNX type 1 and TEs. For some call cases the functional groupings may be null (i.e., they provide no functionality). The dashed rectangle shows one possible implementation of the VPN service.

The originating TE and the terminating TE which are connected to the public VPN service may be served by an a1 service entry point or an a2 service entry point. Whilst an a3 service entry point is not shown, it is not precluded.

Figure 10 should be read from the left (originating functionality) to the right (terminating functionality) for call examples as follows:

a) for a call between two terminals attached to two different PTNXs of type 1, the call passes through the originating PTNX type 1, to the "public VPN service" functional grouping which routes the call to the terminating PTNX type 1, and then to the "terminating TE". Only services that are supported by "public VPN service" may be used by the users attached to PTNX type 1. The so called concatenated scenario (see ETS 300 475-1 [8]) is used;

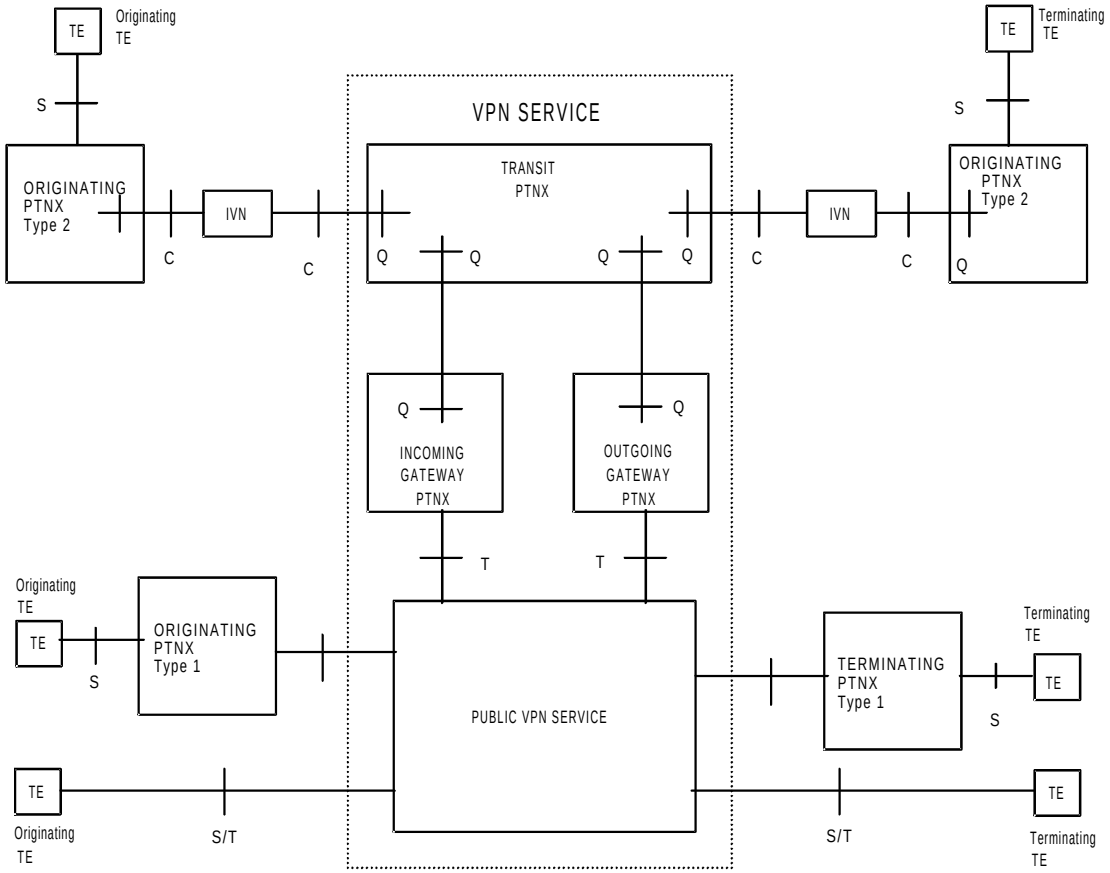


Figure 10: Structural overview showing connection of PTNX type 2

b) for a call from a terminal attached to a PTNX type 1 to a terminal connected to a PTNX type 2, the call passes though an originating PTNX type 1, and is routed via the "public VPN service" to the "gateway PTNX" functional grouping. The "gateway PTNX" performs all service interworking functions between the "public VPN" service and PTN equivalent service. The call then proceeds via the transit PTNX to the terminating PTNX type 2, and then to the "terminating TE".

Other call examples follow the same principles as described for the above two examples.

For non-registered CN access considerations similar to the ones in subclause 7.2.3 apply.

8 Networking aspects - requirements

8.1 Introduction

As described in clause 6 of this TCR-TR, there are two types of PTNXs. The requirements listed in the subsequent subclauses, except subclauses 8.2.4 and 8.3.4 refer only to PTNX type 2.

The interworking of PTNXs type 1 with the public network via the T reference point will be dealt with during the standardization work for VPN services in TC NA and TC SPS by means of the existing practices (see ETS 300 345 [6]).

The requirements stated in subclauses 8.2.4 and 8.3.4 are applicable to both types of PTNXs.

8.2 Emulation of transit PTNX functionality in the public network

This subclause addresses some requirements for the emulation of transit PTNX functionality in the public network.

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 of the transit PTNX functionality are analyzed according to the following components:

- basic call functionality;
- generic functional procedures for the support of supplementary services; and
- supplementary service requirements.

The requirements for each of the above will be identified in subclauses 8.2.1 to 8.2.3.

8.2.1 Basic call requirements

ETS 300 171 [1] defines the stage 1 and 2 requirements for the support of circuit-mode basic services in a PTN.

Transit PTNX functionality needs to satisfy the stage 1 requirements of clauses 4 to 9 of ETS 300 171 [1]. The requirements in this standard need to be taken into account by the relevant ETSI TCs.

In addition, transit PTNX functionality needs to satisfy the requirements outlined in scenarios 1.3, 1.4, 2.3, 3.3, 4.3 and 4.4 of table 10, clause 16 in ETS 300 171 [1]. The functions and information flows to be supported are described in the appropriate clauses of the stage 2 description.

8.2.2 Generic functional procedures for the support of supplementary services requirements

ETS 300 239 [5] defines the generic functional protocol for the support of supplementary services. In particular, it provides the means to exchange signalling information for the control of supplementary services over the PTN. It does not in itself control any supplementary service but rather provides generic service to supplementary service control entities.

Transit PTNX functionality consists of a number of functions as defined in ETS 300 239 [5]. These requirements are identified in the following subclauses. The requirements in this standard need to be taken into account by the relevant ETSI TCs.

8.2.2.1 Transport of supplementary service Information

On receipt of supplementary service related information flows, the transit PTNX function needs to be able to determine whether it is the intended receiver of that information.

If the transit PTNX function determines that it is not the intended receiver of the received supplementary service information flows, the transit PTNX function needs to be able to convey those information flows unchanged to the next PTNX.

If the transit PTNX function is required to provide source PTNX functionality for supplementary service information flows, the transit PTNX function needs to be able to indicate the intended receiver PTNX function for that information.

8.2.2.2 Transit PTNX function is the intended receiver of supplementary service information

When the transit PTNX function is the intended receiver of supplementary service information flows and the information is not recognized, the transit PTNX function needs to be able, when required, to:

- indicate rejection of the supplementary service information to the originator of the information; and

- indicate rejection of the supplementary service information to the originator of the information and clear the associated call.

8.2.2.3 Support of remote operations

The transit PTNX function emulated in the public network needs to support the remote operation functions identified in CCITT Recommendation X.219 [16] for sending and receiving supplementary service information. The requirements in this Recommendation need to be taken into account by the relevant ETSI TCs.

8.2.2.4 Support of protocol functions

ETS 300 239 [5] provides mechanisms for the support of supplementary services which relate to both basic calls or are entirely independent of any basic calls. In performing a particular supplementary service, whether call independent or call related, use may be made of either the call related or the call independent information transfer procedures as appropriate.

The requirements in this standard need to be taken into account by the relevant ETSI TCs.

Where a transit PTNX function is required to receive and/or send supplementary service information flows the protocol to be used needs to be able to convey:

- supplementary service information;
- information identifying the intended receiver of the supplementary service information; and
- information concerning treatment of unrecognized supplementary service information flows,

in equivalent call control information flows to those identified in ETS 300 239 [5].

8.2.2.4.1 Requirements for call related supplementary services information transport

The support of call related supplementary SIT is a mandatory requirement of ETS 300 239 [5].

The protocol to be used to send and/or receive supplementary service information needs to be able to support at least equivalent functions to those described in ETS 300 239 [5].

8.2.2.4.2 Requirements for non-call related supplementary SIT

The support of non-call related supplementary SIT is an optional requirement of ETS 300 239 [5] and may optionally be implemented by a transit PTNX emulated in the public network. Two sets of generic procedures have been defined for the support of non-call related supplementary services, non-call related connection oriented and non-call related connectionless procedures.

a) Non call related connection oriented service requirements

Where this service is provided by a transit PTNX function, the protocol to be used to send and/or receive supplementary service information needs to be able to support at least equivalent functions to those described in ETS 300 239 [5].

b) Non call related connectionless service requirements

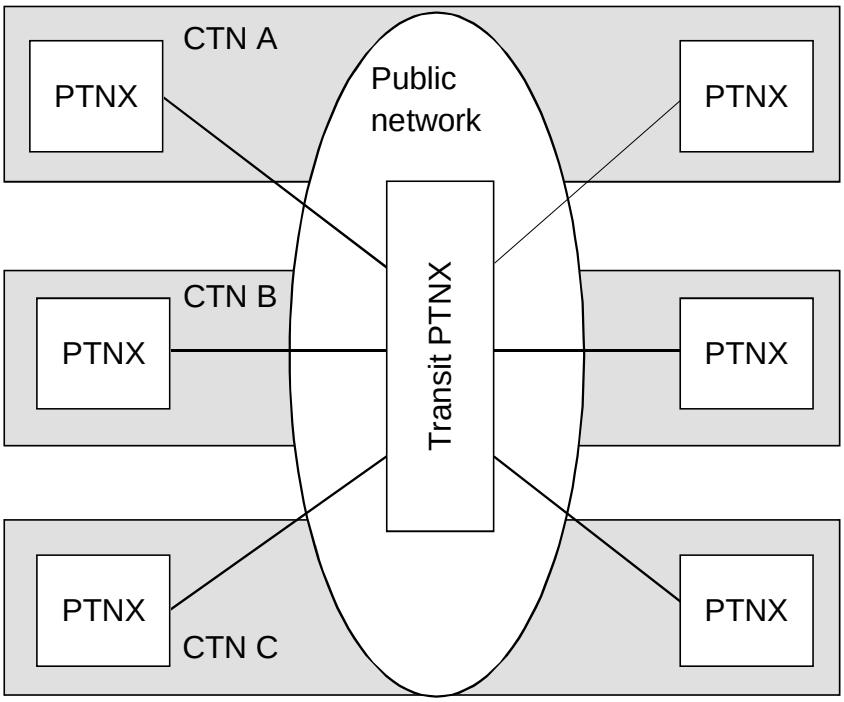
Where this service is provided by a transit PTNX function, the protocol to be used to send and/or receive supplementary service information needs to be able to support at least equivalent functions to those described in ETS 300 239 [5].

8.2.3 Supplementary service requirements

The support of one or more supplementary service procedures defined for the CN by a transit PTNX functions is optional. Where support of a CN supplementary service is required, transit PTNX functionality needs to satisfy the requirements defined for stage 1 and 2 of that supplementary service. In order to support a supplementary service the requirements in this corresponding standard need to be taken into account by the relevant ETSI TCs.

8.2.4 Support of multiple CNs

The public network may be able to 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. An example of such a situation is illustrated in figure 11.



NOTE: "CTN" should be read as "CN".

Figure 11: Support of multiple CNs in a public network

As it can be seen from figure 11, the facilities of the virtual transit PTNX are shared between the three CNs. Thus, the virtual transit PTNX needs to be able to provide differentiation between the calls belonging to the different CNs.

The minimum requirement of the virtual transit PTNX is to be able to uniquely identify the CN to which a particular attached PTNX 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.

Appropriate charging of a particular call as well as appropriate management mechanisms have to be provided.

NOTE: For example, such a mechanism may be based upon the use of non-overlapping numbering plans in each CN or on a piece of information in the PNP which determines the CN involved in the call. In the first case, a limitation is placed on numbering plan capacity. In the second case, its capacity would be less restricted.

8.3 Emulation of gateway PTNX functionality in the public network

This subclause identifies the requirements for the emulation of Private Telecommunication Network (PTN) functionality in the public network. Specifically, this subclause addresses the requirements for the emulation of gateway PTNX functionality in the public network.

NOTE: The requirements identified here are not required 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 of the gateway PTNX are analyzed according to the following components:

- basic call functionality;
- generic functional procedures for the support of supplementary services; and
- supplementary service requirements.

The requirements for each of the above will be identified in the following subclauses.

8.3.1 Basic call requirements

ETS 300 171 [1] defines the stage 1 and 2 requirements for the support of circuit-mode basic services in a PTN.

Gateway PTNX functionality needs to shall satisfy the stage 1 requirements of clauses 4 to 10 of ETS 300 171 [1].

In addition, gateway PTNX functionality needs to satisfy the requirements outlined in scenarios 2, 3 and 4 of table 10, clause 16 in ETS 300 171 [1]. The functions and information flows to be supported are described in the appropriate clauses of the stage 2 description.

The requirements in this standard need to be taken into account by the relevant ETSI TCs.

8.3.2 Generic functional procedures for the support of supplementary services requirements

ETS 300 239 [5] provides the means to exchange signalling information for the control of supplementary services over the PTN. It does not in itself control any supplementary service but rather provides generic service to supplementary service control entities.

Depending upon the capabilities of the network being inter-worked, the gateway PTNX can provide either transit PTNX or end PTNX functionality in the context of the supplementary service concerned. That is, it can either convey information flows unchanged to or from the other network (transit PTNX functionality), or process the information flows and perform an interworking function to the equivalent information flows in the other network (end PTNX functionality).

The functions to be supported when the gateway PTNX is acting as a transit PTNX or end PTNX are described in the following subclauses.

8.3.2.1 Gateway PTNX provides transit PTNX functionality

The requirements identified in subclauses 8.2.2.1 to 8.2.2.6 are applicable.

8.3.2.2 Gateway PTNX provides end PTNX functionality

In the case where a gateway PTNX provides end PTNX functionality, it may be required to provide source and/or destination PTNX functionality. In this case, the requirements identified in subclauses 8.2.2.3 to 8.2.2.6 are applicable. The additional requirements for the source and destination PTNXs are described in the following points:

8.3.2.2.1 Gateway PTNX provides source PTNX functionality

If the transit PTNX is required to provide source PTNX functionality for supplementary service information, the transit PTNX function needs to be able to indicate the intended receiver PTNX function for that information. The intended receiver can be either:

- destination PTNX;
- originating PTNX;
- addressed PTNX; or
- next PTNX.

8.3.2.2.2 Gateway PTNX provides destination PTNX functionality

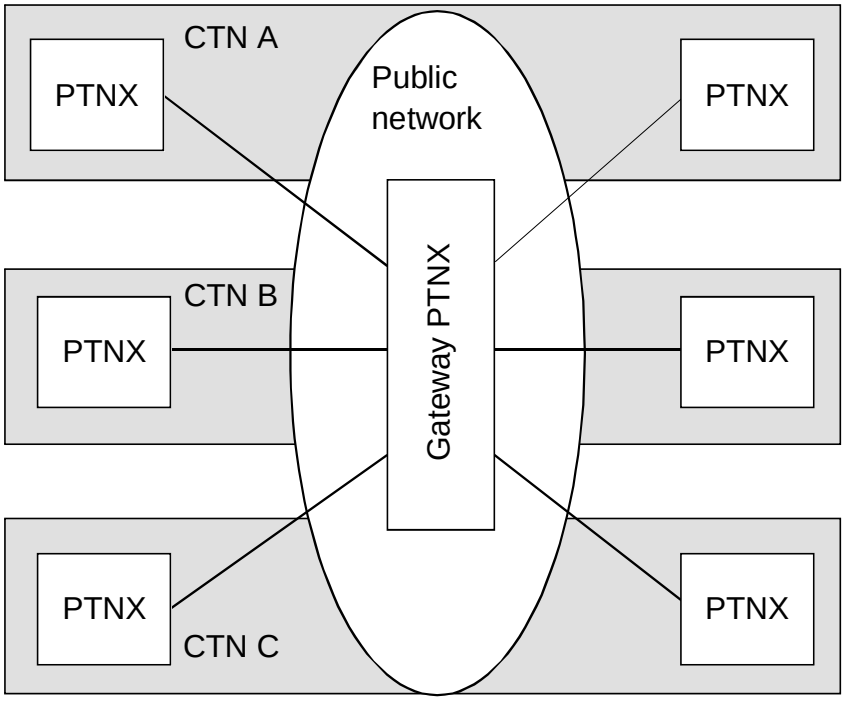
The requirements of subclause 8.2.2.2 are applicable.

8.3.3 Supplementary service requirements

The support of one or more supplementary service procedures defined for the CN by a gateway PTNX emulated by the public network is optional. Where support of a CN supplementary service is required, and depending upon whether the gateway PTNX is providing transit PTNX or end PTNX functionality in the context of the service, a gateway PTNX in the public network needs to satisfy the relevant requirements defined for stage 1 and 2 of that supplementary service.

8.3.4 Support of multiple CNs

The public network needs to support the co-existence of multiple CNs in parallel. That is, the resources of the public network are shared by multiple CNs. Each CN should be considered as a separate network. An example of such a situation is illustrated in figure 12.



NOTE: "CTN" should be read as "CN".

Figure 12: Support of multiple CNs in a public network

As it can be seen from figure 12, the facilities of the virtual gateway PTNX are shared between the three CNs. Thus, the virtual gateway PTNX needs to be able to provide differentiation between the calls belonging to the different CNs.

The minimum requirement of the virtual gateway PTNX is to be able to uniquely identify the CN to which a particular attached PTNX 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.

NOTE: For example, such a mechanism may be based upon the use of non-overlapping numbering plans in each CN or on a piece of information in the PNP which determines the CN involved in the call. In the first case, a limitation is placed on numbering plan capacity. In the second case, its capacity would be less restricted.

8.4 Emulation of originating and/or terminating PTNX functionality in the public network

This subclause identifies the requirements for the emulation of originating and/or terminating PTNX 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.

8.4.1 Service assumptions

The provision of CNs is a competitive service.

The standardization process should not be used to inhibit innovation or the deployment of new or enhanced services.

However, some standardization is required to meet the following aims:

- an adequate level of interworking between private and public ISDN services, where the terminals which provide these services have to operate in a "multi-vendor" type market; and

- for interoperability within the private networks for private network services and related protocols, which will allow a multi-vendor environment (from a user point of view) with regard to terminals, PBXs and Centrexes.

These aims have resulted in the mandated work orders BC IT-74 to BC IT-77 (see annex G).

Since some of the more important corporate networks are global rather than regional there is a preference for global standards.

8.4.2 Connection requirements

Four types of network connections can be identified:

a) connection to an PBX;
b) connection through the CN;
c) access from a digital terminal; and
d) access from an analogue terminal.

8.4.2.1 Connection to a PBX

The interface here is the same as that between two PBXs.

8.4.2.2 Connection through the CN

It is not intended to make any recommendations.

8.4.2.3 Access from a digital terminal

The reference point here is an "S" reference point as shown in figure 1. The following standards are the only ones which apply at the S reference point:

ETS 300 190 [2]	Generic stimulus procedure for the control of supplementary services using the keypad at the S reference point.
ETS 300 191 [3]	Protocol for signalling over the D-Channel of interfaces at the S reference point between terminal equipment and PTNs for the support of identification supplementary services.
ETS 300 192 [4]	Layer 3 protocol for signalling over the D-Channel of interfaces between terminal equipment and PTNs for the control of circuit-switched calls.

Whether further standards are required is a regulatory issue. The attachment of terminals to CPE, e.g. an PBX, does not normally attract regulatory interest whereas the attachment of CPE to Centrex is likely to do so.

8.4.2.4 Access from an analogue terminal

This interface is outside the scope of the terms of reference of this task group. The TG will recommend the ETSI should not standardize access protocols at Centrex nodes for analogue terminal equipment.

8.5 Support of a CN spanning multiple public networks

According to the reference model given in subclause 7.1, a CN can consist of equipment located in more than one public network. To perform CN services it is required that all the information flows as described in subclauses 7.1 to 7.3 are supported via the interface between the different public networks. Additionally the requirements derived from subclauses 7.2.5 and 7.2.6 as e.g. the possibility to identify a specific CN need to be fulfilled.

The following considerations have to be taken into account at this interface.

It was recognized that authorization codes has no impact on the international interface because each network contains all the security mechanisms associated with the user belonging to that network, and because authorization codes are realized by means of local validation.

In the same way, the support of CN access for individual users and non-registered CN access has no impact on the international interface because each network contains all the data necessary to realize it.

The following possible impacts on the international interface have been recognized:

- when both networks (originating and destination) have to check those calls in which both networks (originating and destination) need to determine user privileges and restrictions such as, for example, identification of the CN implied in the call on the specific groups of CN users that benefit from a certain service;

- when calls need an alternative route to complete the call because of congestion, or because they are based on a predetermined situation (time, day, origin, etc.)

- in the case of "incoming call screening".

    NOTE: Since "outgoing call screening" only requires information associated with the calling party, thus the network implied in this control will be the original network.

However, other requirements may impact the international interface. this will need further study.

There can be two configurations of interconnected public networks, namely:

a) the public networks are located in different countries and are interconnected via the international interface;

b) the public networks are located within one country and are interconnected via an interface different from the international interface.

    NOTE: Theoretically, they can also be connected via the international interface in which case items a) and b) coincide.

This TCR-TR is only applicable for item a) because if the interface between the public networks is nationally agreed and not subject to standardization the functionality to perform CN services cannot be guaranteed on that interface.

8.6 Support of CN management

This item will be examined in an ETSI task group consisting of delegates of ETSI STC NA1 and ECMA TC32. The results will be reported to ETSI TA.

8.7 Support of CN access for individual users

Users in a CN will access the services of the CN in a number of ways depending on how their terminal equipment is connected to the CN. Such connections to the CN may be physical or logical.

The following access arrangements for users have been identified:

a) a user connected to a PBX;
b) a user connected to the public network, but whose access is considered as being a CN access;
c) a user connected to the public network, but whose access is registered as having access to a CN; and
d) a user connected to the public network, without any association with a CN.

Item a) has only been included for completeness.

    NOTE: For each of items b) to d), security mechanisms may need to be employed to prevent fraudulent use.

8.7.1 Users connected to the public network, but whose access is considered as being a CN access

Users connected according to subclause 8.7, item b) are CN users, and are logically part of a CN. An example would be users in a CN who are located on small sites. Such users would be supported using "Centrex" type solutions.

These users will be able to make calls within the CN as for a user connected to a PBX. Calls into the public network will be made by indicating that a public network call is required.

8.7.2 Users connected to the public network, but whose access is registered as having access to a CN

Users connected according to subclause 8.7, item c) are public network users, and will normally make public network calls.

Such users can make calls within the CN by means of some service request which identifies those calls to the public network. On doing this, the user is considered as a CN user for that call. Subclause 7.2.3 and figure 4 give more details.

Examples of such access arrangements include teleworking where the user uses their home telephone which is normally a "public network telephone" to make calls as a user on a CN.

8.7.3 Users connected to the public network, without any association with a CN

In this case, the CN has no knowledge of the user and procedures will be necessary to enable the user to temporarily register with the CN.

The user will need to identify the CN to which they wish to be connected and also to provide some identification of who they are so that the correct user profile may be assigned.

On registering with the CN and being given a service profile, the user would be treated as a CN user for the duration of the temporary registration. Subclause 7.2.3 and figure 4 give more details.

This mechanism could be used by service engineers or salesmen who are visiting customers and wish to use the services of their own CN (e.g. having their calls billed to their own company's account, or using their own service profile to gain access to computer facilities).

It is strongly recommended that security measures are employed in order to prevent fraudulent use of this method of access.

8.8 Network performance parameters related to CN

8.8.1 Transmission performance

For further study.

8.8.2 Guidelines for grade of service performance

For further study.

9 Networking aspects - work plan

Work item 7:	Study of signalling protocols at the international interface to support VPN services across multiple public networks and interconnection of different VPN service providers.
Responsible TC:	SPS
Interested TCs/STCs:	NA6
Description:	SPS should study all the necessary enhancements of Signalling System No.7 (SS7) protocols in order to support the VPN services spanning multiple public networks and multiple VPN service providers.

Work item 8:	Specification of the protocol for the provision of VPN services to end users (a service entry points).
Responsible TC:	SPS
Interested TCs/STCs:	ECMA TC32
Description:	It is necessary to identify network solutions to provide end users with the services which will be defined at the a service entry points. The service descriptions will be developed by NA.

Work item 9:	Identification and specification of a suitable protocol to support VPN services to PBXs (b service entry point).
Responsible TC:	SPS
Interested TCs/STCs:	ECMA
Description:	It is necessary to identify network solutions to provide PBXs with the services which will be defined at the b service entry point. The service descriptions will be developed by NA. PTNX type 1 and PTNX type 2 need to be supported. SPS should study the improvements which are possible in the Digital subscriber Signalling System No. 1 (DSS1) and in QSIG (in conjunction with ECMA) in order to obtain a single protocol between PTNXs and public network equipment.

Work item 10:	Identification of requirements of an inter PTNX signalling protocol to support VPN services available at the b service entry point.
Responsible TC:	ECMA
Interested TCs/STCs:	SPS
Description:	This work item relates only to the protocol used on a link between PTNXs which does not utilize the VPN service i.e. the work item is not applicable to the protocol used at the b service entry point. ECMA should consider all the necessary improvements to the QSIG protocol resulting from work item 9.

Annex A: Supplementary services for public networks (studied by ETSI STC NA1)

Table A.1 has been produced from information in ETR 076 [9].

Table A.1

Acronym	Supplementary service
AOC-S	Advice of Charge (at call set-up)
AOC-D	Advice of Charge (during the call)
AOC-E	Advice of Charge (at the end of the call)
CD	Call Deflection
CFB	Call Forwarding Busy
CFNR	Call Forwarding No Reply
CFU	Call Forwarding Unconditional
HOLD	Call Hold
CW	Call Waiting
CLIP	Calling Line Identification Presentation
CLIR	Calling Line Identification Restriction
CCC	Charge Card Calling
CUG	Closed User Group
CCBS	Completion of Calls to Busy Subscriber
CONF	Conference call, add On
COLP	Connected Line Identification Presentation
COLR	Connected Line Identification Restriction
DDI	Direct Dialling In
ECT	Explicit Call Transfer
FPH	Freephone
IM	In-call Modification
LHTH	Line Hunting/Trunk Hunting
MCID	Malicious Call Identification
MMC	Meet Me Conference
MSN	Multiple Subscriber Number
OCB	Outgoing Call Barring
PRM	Premium Rate
RCSS	Remote Control of Supplementary Services
REV-S	Reverse Charging (call Set-up)
REV-U	Reverse Charging (Unconditional)
SCFB	Selective Call Forwarding Busy
SCFNR	Selective Call Forwarding No Reply
SCFU	Selective Call Forwarding Unconditional
SUB	Subaddressing
SPNP	Support of Private Number Plan
VOT	Televoting
TP	Terminal Portability
3PTY	Three Party
UAN	Universal Access Number
UUS	User-to-User Signalling
VCC	Virtual Card

Annex B: Supplementary services for private networks (studied by ECMA TC32 and JTC1 ISO/IEC SC6)

Table B.1 has been produced from information in ETR 076 [9].

Table B.1

Acronym	Supplementary service
AIP	Additional Information Presentation
AOC-S	Advice of Charge (at call set-up)
AOC-E	Advice of Charge (at end of call)
AOC-D	Advice of Charge (during call)
CD	Call Deflection
CDA	Call Distribution to Attendant
CFB	Call Forwarding Busy
CFNR	Call Forwarding No-Reply
CFU	Call Forwarding Unconditional
HOLD	Call Hold
CO	Call Offer
CW	Call Waiting
CLIP	Calling Line Identity Presentation
CLIR	Calling Line Identity Restriction
CNIP	Calling Name Identity Presentation
CNIR	Calling/Connected Name Identity Restriction.
CCNR	Completion of Calls on No-Reply
CCBS	Completion of Calls to Busy Subscriber
CONF	Conference Call Add On
COLP	Connected Line Identity Presentation
COLR	Connected Line Identity Restriction
CONP	Connected Name Identity Presentation
CDIV	Controlled Diversion
CDIVC	Controlled Diversion Consult
DDI	Direct Dialling In
DND	Do Not Disturb
DNDO	Do Not Disturb Override
ECT	Explicit Call Transfer
IM	In-call Modification
INTR	Intrusion
LHTH	Line Hunting/Trunk Hunting
MPA	Multi Private ISDN Attendant
MSN	Multiple Subscriber Number
NIMT	Network Interception
NS	Night Service
OCB	Outgoing Call Barring
RE	Recall
RCSS	Remote Control of Supplementary Service
SC	Serial Call
SUB	Subaddressing
SIP	Supervisory Information Presentation
SPNP	Support of Private Number Plan
TP	Terminal Portability
UUS	User-to-user Signalling
ANF-ARI	ANF Alternate Routeing Indication
ANF-C	ANF Common Information
ANF-PR	ANF Path Replacement
ANF-RR	ANF Route Restriction
ANF-SR	ANF Source Routeing

Annex C: GVNS service features (studied by ITU-T SG1 and ETSI STCs NA1/NA6)

Table C.1 identifies the GVNS service features as of end of 1993.

Table C.1

Acronym	Service feature
ABD	Abbreviated Dialling
ACC	Accounting Code
AD	Alternate Destination on Busy/No-Reply
ATT	Attendant
AUTH	Authorization Code
CFU	Call Forwarding Unconditional
COAMP	Centralized Operation, Administration, Maintenance and Provisioning
CPM	Customer Profile Management
CRA	Customized Recorded Announcements
CSCR	Call Screening
HOT	Hotline
LOG	Call Logging
ODR	Origin Dependent Routeing
PUB	Public Number
SPD	Speed Dialling
STAT	Statistical Information
SUBN	Sub-Networking
TDR	Time Dependent Routeing

Annex D: Centrex in different VPN scenarios

This annex contains a number of implementation scenarios (not exhaustive). It is included for information purposes. The choice of a particular scenario is outside the scope of this TCR-TR.

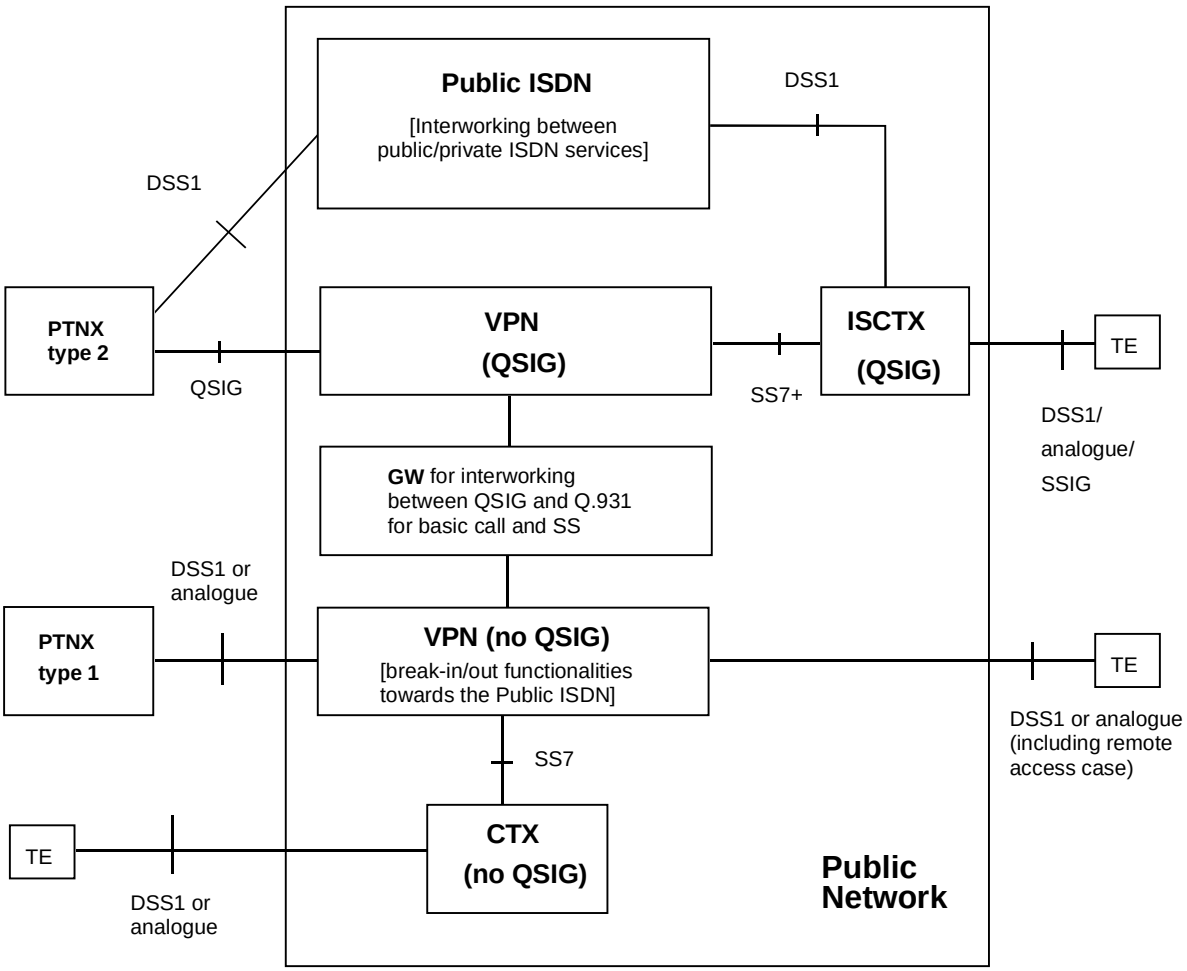
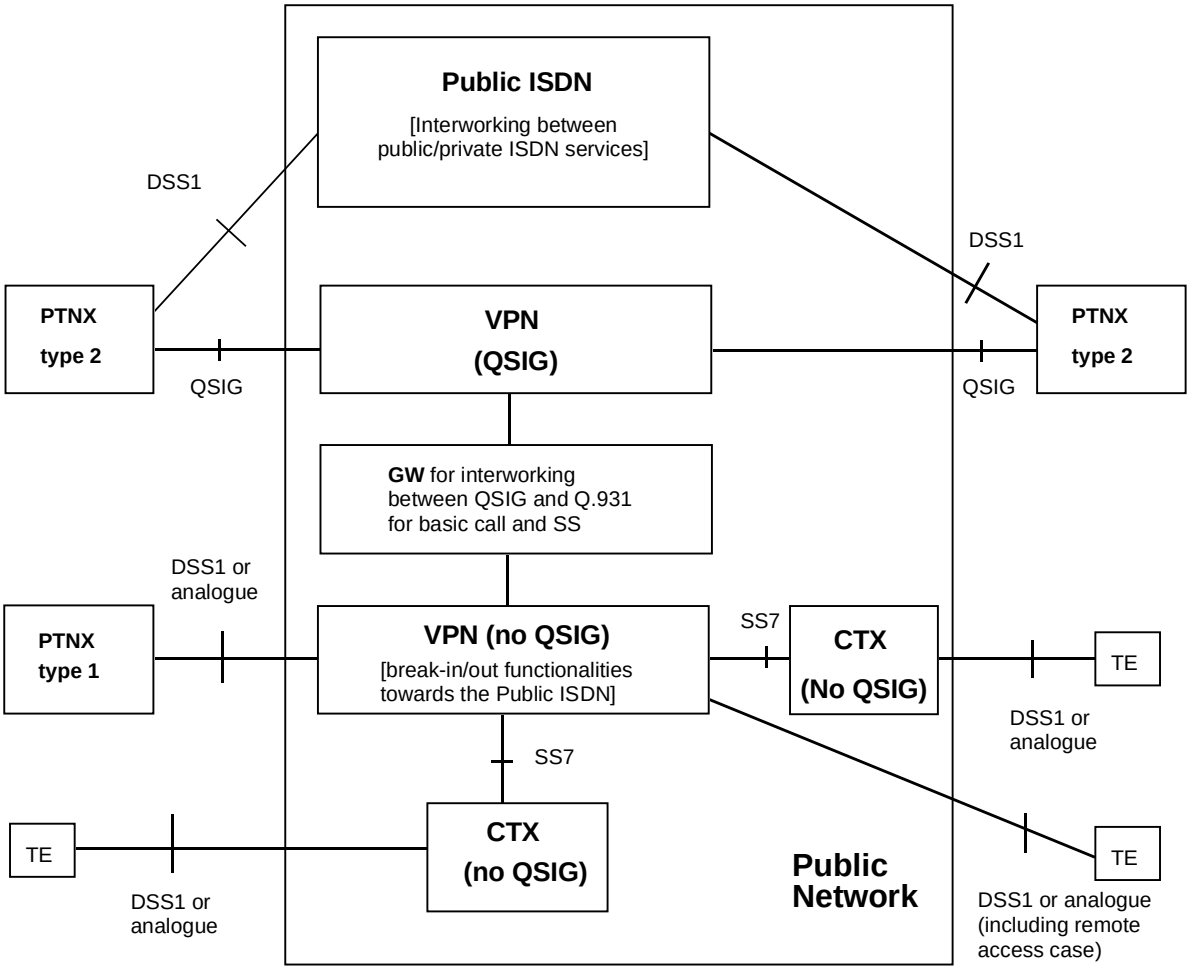


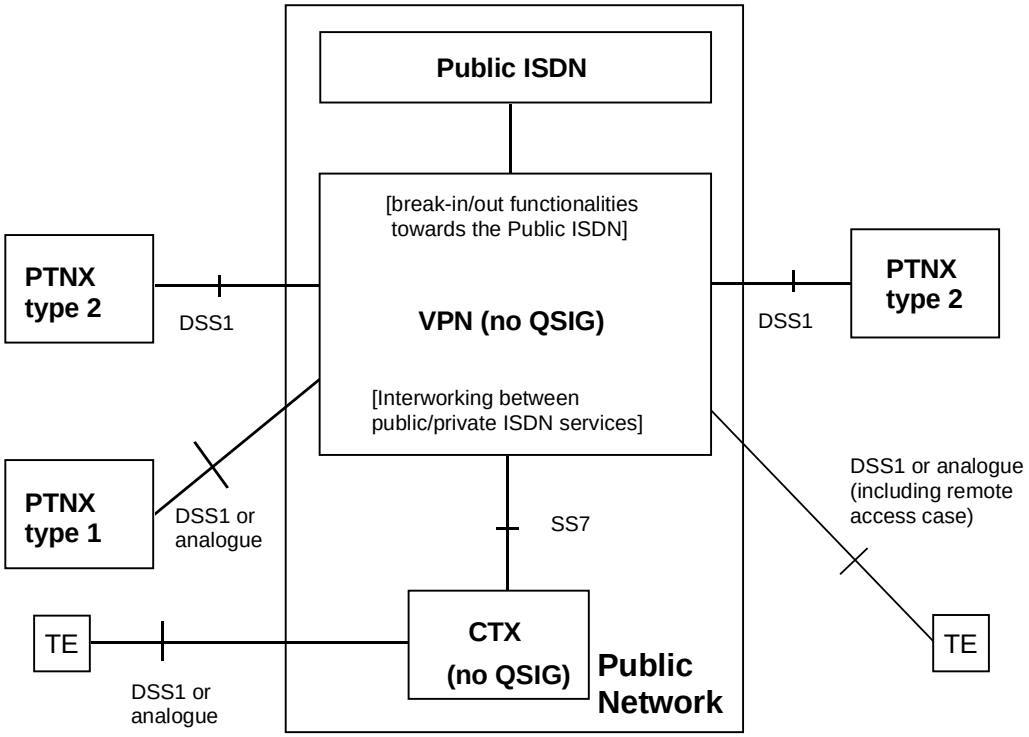
Figure D.1: VPN scenario 1

In scenario 1, no standardization activities are necessary for the Integrated Services CenTralized eXchange (ISCTX) (QSIG), since the ECMA/ETSI standards for PTNs apply.



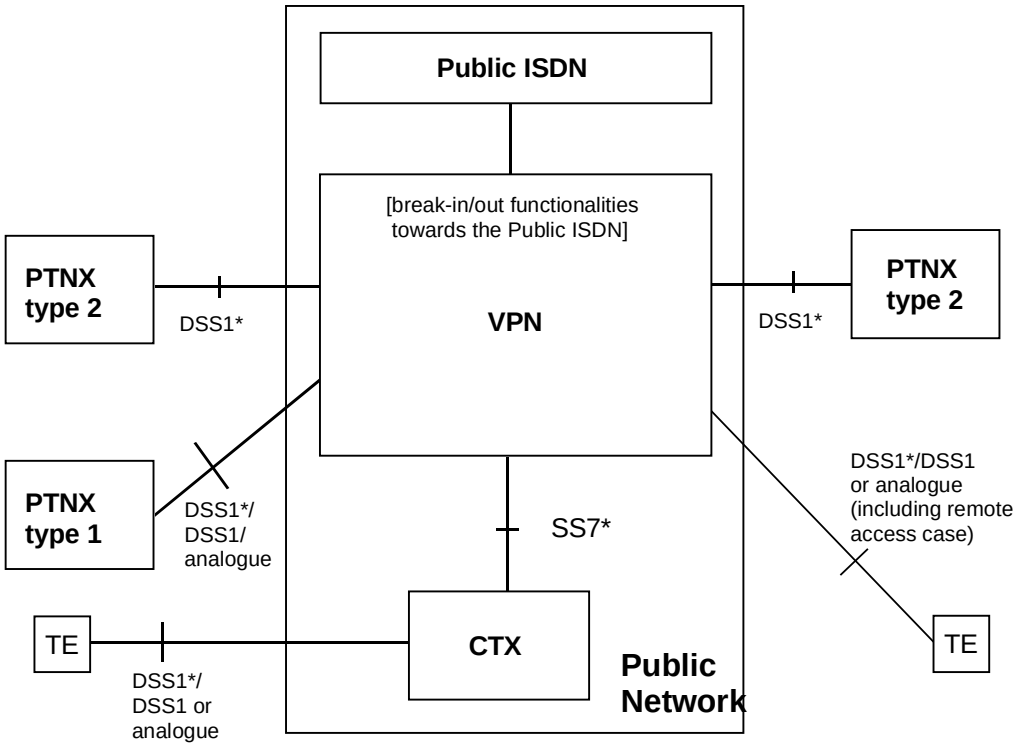
NOTE: For the CenTralized eXchange (CTX) (no QSIG), (a) Technical Report(s) could be produced covering the description of new "end-to-end" services for wide-area Centrex solutions. For some of the ECMA/ETSI PTN supplementary services, the development of a public version of the service, "harmonized" with the standardized private version (at least for the stage 1 and 2 service descriptions) could be considered.

Figure D.2: VPN scenario 2



NOTE: The note in figure D.2 (VPN scenario 2) applies.

Figure D.3: VPN scenario 3

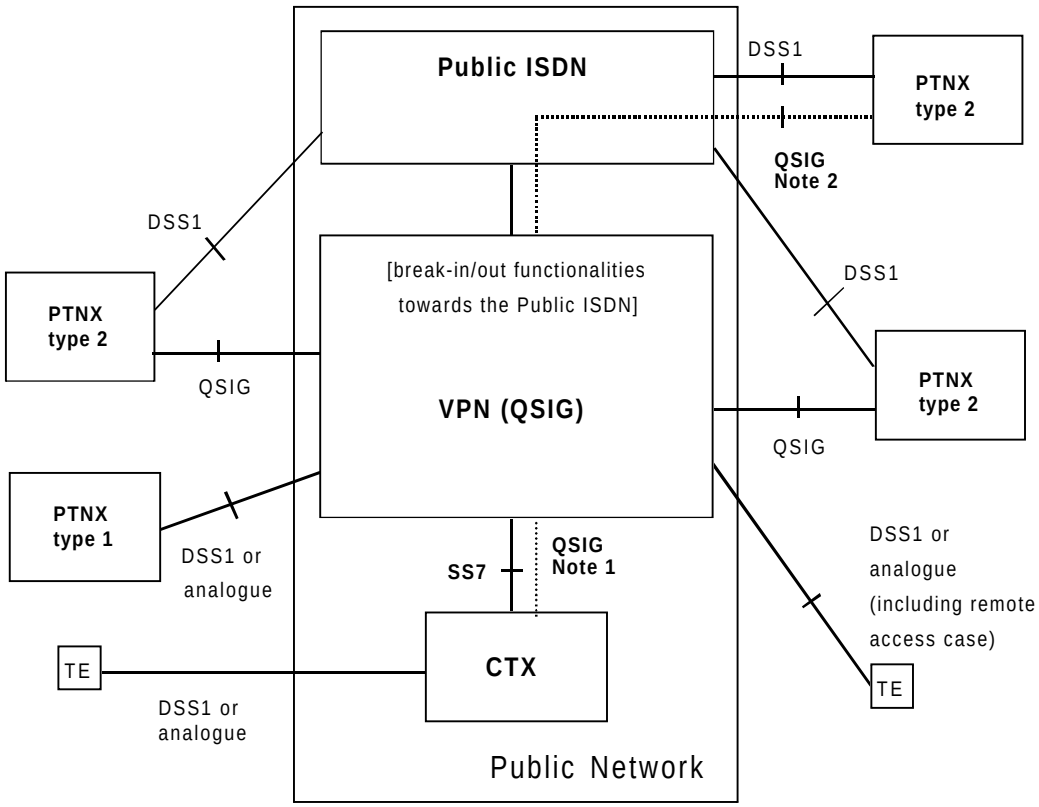


NOTE: The note in figure D.2 (VPN scenario 2) applies.

Figure D.4: VPN scenario 4

The term "DSS1*" indicates an enhanced DSS1 protocol, that is backward compatible with DSS1, in order to support ECMA/ETSI PTN services (for basic call and supplementary services). An example of a "DSS1*" protocol is the I-CAN solution being developed by Bellcore.

The development of a protocol of an enhanced DSS1 protocol will let a CTX, also in wide-area solution, to offer its users: public ISDN services, private ISDN services, harmonized public and private ISDN services, PSTN services, proprietary services.



NOTE 1: The QSIG information flows are carried by a suitable SS7 mechanism (i.e. the overlay scenario).

NOTE 2: Overlay scenario.

Figure D.5: VPN scenario 5

Annex E: VPN management services

In this annex, a set of VPN management services is briefly described. This set is not meant to be exhaustive but just to give an overview of the VPN management concept.

Each VPN management service is described in terms of its activity.

- single point of contact;
- VPN data management;
- performance management;
- fault management;
- security management;
- customer control procedures;
- supervisory management service;
- management of CN numbering plans;
- routeing administration;
- customized recorded announcements;
- call logging;
- statistical information on calls;
- flexible billing.

E.1 Single point of contact

This feature, useful in the case of VPN services offered by a single VPN service provider, is particularly useful when a VPN involves different VPN service providers belonging to the same country or to different countries. It is essential for the VPN service subscriber to have a single point of reference (called "VPN service provider co-ordinator") to face for any issue regarding their CN. The VPN service subscriber shall be able to choose, among the VPN service providers involved for the VPN service offering, the VPN service provider to act as the "VPN service provider co-ordinator". For issues local to a VPN service provider, the VPN service subscriber will be able to address the local VPN service provider (who will be able to communicate with all the other local VPN service providers, involved for the service offering). The same organizational model could be used by the VPN service subscriber, who could elect a "VPN customer co-ordinator" able to directly address the "VPN service provider co-ordinator".

E.2 VPN data management

The VPN service subscriber may have access, also with customer control procedures, to the following configuration data for their VPN services:

- CN numbering plans and routeing configuration;
- allocation of physical resources;
- service provisioning data (e.g. related to variable destination, remote access).

A VPN service subscriber may as a subscription option be given access to different management functions for the management of all or a limited set of the configuration data. There may also be different access privileges to the data, e.g. to read only, or modify allowed.

E.3 Performance management

The VPN performance management functionalities enable the VPN service provider to manage performance of the VPN resources and report to the VPN service subscriber whether required. performance management provide functions to evaluate and report upon the behaviour of telecommunication equipment and on the effectiveness of the VPN. The performance management role is to gather statistical data for the purpose of monitoring and correcting the behaviour and effectiveness of the CN, and to aid in the planning and analysis phases. Performance management functionalities may cover the following aspects:

- performance monitoring;
- traffic measurement;
- status monitoring functions;
- control functions; and
- quality of service observations.

Performance information can also be provided to the VPN service subscriber by means of customer control procedures.

E.4 Fault management

The fault management functions enable the VPN service provider to manage access faults, exchange faults (including databases and service logic aspects) and provide means to inform the VPN service subscriber about faults and corrections. Fault (maintenance) management is a set of functions which enables the detection, isolation and correction of abnormal operation of the VPN and its environment. Fault management functionalities may cover the following aspects:

- alarm surveillance;
- fault location;
- testing; and
- statistical information on alarms/faults.

Fault information can also be provided to the VPN service subscriber by means of customer control procedures.

E.5 Security management

The security management functionalities enable the VPN service provider to manage security aspects and to provide the VPN service subscriber with:

- security means for the transfer of private signalling information across the VPN;
- secure databases: all kind of possibilities (technical solutions) to reach this goal have to be used for software, hardware and communication procedures;
- secure service deployment and procedures; and
- security aspects in connection with possibilities for the VPN service subscriber to control service profiles with customer control procedures.

E.6 Customer control procedures

In this VPN management service the VPN service subscriber is allowed to interact with the management system of the VPN. This will enable the manageable aspects of the VPN configuration to be accessed by the VPN service subscriber directly and provide reports on network resources currently allocated to the VPN. Thus a VPN service subscriber may change his own configuration within the limits allowed by the VPN service provider. This may mean increasing or decreasing the range of VPN services available, subject to VPN performance/policy evaluations and with consequent billing arrangement amendments.

E.7 Supervisory management service

Supervisory Information Presentation (SIP) provides for the presentation of supervisory information to the attendants of telecommunication networks. The information provided is not related to any specific call but is of a general nature, providing attendants with additional information on the operational status of the VPN. The SIP information is packaged as a supplementary service and is provided by the same mechanism as is used to support customer control procedures, and in many instances is similar to information presented at management interfaces. For this reason SIP is considered from a management perspective. SIP provides for a "read only" access to information. VPN management is used to provide this access and set operational parameters.

E.8 Management of CN numbering plans

This management service allows the VPN service provider to offer the support of private numbering plans to the VPN service subscriber. This management service also allows the VPN service provider to allocate a range of admissible values to each numbering plan and to allocate the individual number values to addressable entities.

The CN numbering plans can also be changed by means of customer control procedures.

E.9 Routeing administration

The purpose of management of routeing information in a VPN is to allow a VPN service provider to change the VPN routeing information reacting upon the VPN service subscriber requests. In order to provide this service, certain requirements need to be met:

- it should be possible for the VPN service subscriber to verify routeing information in a VPN;
- it should be possible to switch between routeing plans according to a predefined timing schedule; and
- it should be possible to define functionality in such a way that routeing plans may easily be changed.

This service can also be offered by means of customer control procedures.

E.10 Customized recorded announcements

This service allows the VPN service provider to define different announcements for particular call conditions, for instance, unsuccessful call completion due to different reasons (e.g. all lines engaged, called party not available at that time of day, calling party not authorized to make that kind of call, etc.). The VPN service subscriber shall be able to specify the contents of each announcement (e.g. to give special instructions to users) as well as the conditions which the announcements is to be invoked. Announcements are recorded in co-operation with the VPN service provider. This service may be used to route a CN call to a terminating recorded announcement.

E.11 Call logging

This service enables the VPN service subscriber to obtain from the VPN service provider detailed information on calls and/or call attempts placed to the service. The information to be provided may be one or a combination of the following:

- calling party number;
- destination number;
- time and date;
- charge;
- call result (connected, busy, barred, not answered, etc.); and
- any service specific information.

E.12 Statistical information on calls

This service permits the VPN service subscriber to obtain from the VPN service provider statistical information on calls placed to the service. Such information may be for example daily traffic curve, traffic analysis per routeing area, performance evaluation.

This service can make use of call logging functionalities.

E.13 Flexible billing

This feature allows the VPN service subscriber to arrange with the VPN service provider the type of charging and billing for calls originated in the CN.

For example, billing records associated to:

- calling line identities;
- personal identifier numbers;
- account numbers for the CN;
- different sites;
- departments;
- different type of services;

and what type of information that is to be included.

In order to provide this service call logging functions may be necessary.

Annex F: Recommendations for other work

This annex contains recommendations for other studies in the VPN area which are outside the scope of this TCR-TR.

Recommendation 1:	Study of VPN services supported by public networks.
Responsible TCs:	SMG and NA for mobile networks and data networks respectively.
Interested TCs/STCs:	BTC1, ECMA TC32 TG13
Description:	Study of the implementation aspects and service requirements for the VPN services to be provided by public mobile networks and public data networks and identification of requirements on service interworking at the c service entry point for the provision of a VPN service offering that spans the PSTN and public ISDN as well. In order not to delay further standardization of a highly required VPN service in the public ISDN. JTG/VPN recommends that a first standardization activity is limited to the provision of VPN services by the public ISDN with a defined c service entry point for interconnection with other public networks. As the VPN services described above could be provided by other public networks than the public ISDN further studies should be focused on this issue.

Annex G: JTG/VPN mission statement

To identify the impact on standardization activities in the relevant TCs and STCs/TG's of ETSI and ECMA with regard to the subject of VPN. The investigation shall taking account of:

a) Recommendations 34 and 35 contained in the report of SRC4 (see ETSI/TA14(92)29 [14]);

b) the anticipated recommendations relevant to VPN resulting from SRC5 (see ETSI/TA18(93)25 [15]);

c) the results of the VPN workshop meetings; and

d) EC "political" mandate covering the standardization of private networks.

The work of this TG shall consist mainly of translating the above recommendations into public network requirements leading to a standardization framework applicable for VPNs both in Europe and world-wide.

The deliverable shall be a TCR-TR indicating:

- the TCs/STCs/TG's involved;
- the technical issues to be solved;
- the standardization requirements expressed by draft ETSI work items.

Participation in the Task Group is open to all ETSI members. However, as a minimum, the TG shall include one nominated delegate from the following STCs:

ETSI: BTC1, NA1, NA4, NA6, SPS1, SPS2, SPS5; and

ECMA: TC32 TG12, TC32 TG13, TC32 TG14.

Delegates from other STCs are welcomed to participate in the Task Group.

It is expected that the TG activities will be pursued in three working groups in the following areas:

- service aspects;
- network aspects; and
- management aspects.

Annex H: JTG/VPN members

NOTE: Members whose name are preceded by an * attended more than one meeting.

*	Raoul De Noel ALCATEL	Tel.: Fax:	+32 3 240 40 68 +32 3 240 99 99
	Mauro Fallani RACE Industrial Consortium	Tel.: Fax:	+32 2 6748 519 +32 2 6748 538
	Pekka Ylae-Kotola Helsinki Telephone Company	Tel.: Fax:	+358 0 606 4864 +358 0 606 4839
*	Christian Allain ALCATEL CIT	Tel.: Fax:	+33 1 30679325 +33 1 30673458
*	Vincent Devarenne France Telecom (CNET)	Tel.: Fax:	+33 1 45 29 63 15 +33 1 45 29 63 37
*	Catherine Pouvreau France Telecom, CNET	Tel.: Fax:	+33 1 45 29 66 68 +33 1 46 29 31 42
*	Michèle Wittmann France Telecom (CNET)	Tel.: Fax:	+33 1 45 29 43 80 +33 1 46 29 63 37
	R Koxholt Siemens AG, PNSTA1	Tel.: Fax:	+49 89 722 32 058 +49 89 722 23 977
*	Beate Letzas Deutsche Bundespost Telekom	Tel.: Fax:	+49 6151 83 2867 +49 6151 83 6714
*	Wolfgang Lautenschlager Alcatel SEL AG VS/SNN	Tel.: Fax:	+49 711 8217652 +49 711 8213273
	Dieter Müller Telekom	Tel.: Fax:	+49 6151 83 4333 +49 6151 83 4092
*	Barbara Rudnick Siemens AG	Tel.: Fax:	+49 89 722 32788 +49 89 722 32495
*	Axel Stossno Deutsche Bundespost Telekom	Tel.: Fax:	+49 6151 832869 +49 6151 83 4421
*	Harald Theis Telenorma GMBH	Tel.: Fax:	+49 69 7505 3495 +49 69 7505 4354
	Andreas Wurzinger ALCATEL SEL AG	Tel.: Fax:	+49 30 7002 2907 +49 30 7002 2851
	Bergthor Halldorsson PTT Island	Tel.: Fax:	+354 1 636000 +354 1 636209
*	P. Andreoli CSELT	Tel.: Fax:	+39 11 228 5035 +39 11 228 5069
*	Donatella Chiara CSELT	Tel.: Fax:	+39 11 2286956 +39 11 2286909

*	Felice Faraci CSELT	Tel.: Fax:	+39 11 2285573 +39 11 2285520
	Claudio Giliardi CSELT		
	Enrico Lavoro CSELT		
*	Andrea Lazzaroli SIP DG	Tel.: Fax:	+39 6 3688 6407 +39 6 3222 639
	Franco Pensini Italtel		
	Luigi Quattrocchi CSELT		
*	Cinzia Sternini SIP DG	Tel.: Fax.	+39 6 3688 6243 +39 6 3222 637
*	Wouter Franx AT&T NSI	Tel.: Fax:	+31 35 87 23 17 +31 35 87 58 36
	Ruud A.S Willemstein Philips Communication Systems	Tel.: Fax:	+31 35 89 35 99 +31 35 89 31 60
	Cyriel Spruijt Royal PTT Netherlands		
*	Frode Såstad Norwegian Telecom	Tel.: Fax:	+47 22 77 9100 +47 22 95 5735
*	Eloy Agudo Telefonica de España	Tel.: Fax:	+34 1 584 9723 +34 1 584 9558
*	Ascension Leret TELEFONICA de España	Tel.: Fax:	+34 1 584 6927 +34 1 584 6955
*	Greg Barnicoat Ericsson Telecom AB	Tel.: Fax:	+46 8 719 7934 +46 8 719 2701
	Gustav Bergman Telia Research	Tel.: Fax:	+46 40 10 50 22 +46 40 10 51 00
	Rune Boman Telia AB	Tel.: Fax:	+46 8 713 10 16 +46 8 93 68 29
*	Kerstin Erlandsson Telia AB	Tel.: Fax:	+46 8 713 35 14 +46 8 94 78 54
*	Anders Holmström Telia AB	Tel.: Fax:	+46 8 713 18 56 +46 8 713 20 39
	P.-O. Jernberg Telia AB	Tel.: Fax:	+46 8 713 42 57 +46 8 713 13 92

	P.-A. Johansson Telia AB	Tel.: Fax:	+46 8 713 10 00 +46 8 713 15 54
	Robert Khello Ericsson Telecom	Tel.: Fax:	+46 8 719 5523 +46 8 719 0806
	Ivan Kruzela Telia Research	Tel.: Fax:	+46 40 10 50 21 +46 40 10 51 00
*	Gösta Linder Ericsson Telecom AB	Tel.: Fax:	+46 8 719 4802 +46 8 719 0608
	Nils Weidstam Tele2 AB	Tel.: Fax:	+46 8 632 40 20 +46 8 632 42 00
	Mr. N. J. Abbott British Telecom	Tel.: Fax:	+44 473 22 7833 +44 473 22 7884
*	Colin Bates British Telecom	Tel.: Fax:	+44 473 227111 +44 473 227884
	David Batkin BT	Tel.: Fax:	+44 473 227 140 +44 473 227 884
	Stephen Gowland Mercury Communications Ltd	Tel.: Fax:	+44 344 713 842 +44 344 713 015
	Alex Hardisty PQM Consultants	Tel.: Fax:	+44 291 626 180 +44 291 626 190
*	Chris Kemp Ericsson Ltd	Tel.: Fax:	+44 444 234 295 +44 444 234 527
*	Steve Moore GPT Limited	Tel.: Fax:	+44 602 434 988 +44 602 434 992
*	John Scott Northern Telecom Europe	Tel.: Fax:	+44 628 794 417 +44 628 794 034
*	Alwyn Thomas Dept. of Trade & Industry	Tel.: Fax:	+44 71 215 1742 +44 71 931 7194

History

Document history		
January 1995	Draft	For consideration by TCC 19
June 1995	Final draft	Endorsed by TCC 20, for approval by TA
September 1995	First Edition	
June 1996	Converted into Adobe Acrobat Portable Document Format (PDF)	