Draft EN 301 062-1 V1.1.1 (1997-08)

European Standard (Telecommunications series)

Integrated Services Digital Network (ISDN); Signalling System No.7; NNI extensions to support VPN applications

European Telecommunications Standards Institute

Reference

DEN/SPS-01032-1 (9u090ico.PDF)

Keywords

ISDN, SS7, ISUP, TC, VPN, PINX

ETSI Secretariat

Postal address

F-06921 Sophia Antipolis Cedex - FRANCE

Office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16
Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

X.400

c= fr; a=atlas; p=etsi; s=secretariat

Internet

secretariat@etsi.fr
http://www.etsi.fr

Contents

Intellectual Property Rights

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

Foreword

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

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

1 Scope

The present document describes the extensions required for the support of Virtual Private Network (VPN) applications over the public Network Nodal Interface (NNI). This application makes use of the Application Transport Mechanism described in Q.apm for bearer-related signalling, and the Transaction Capability for signalling involving no bearer. The present document specifies the respective users (i.e. APM-user, TC-user) to support the PSS1 information flow continuity in VPN applications. The public NNI provides transparency to the services of the private network.

The private network functionality is defined by ISO in its series of standards for Private Integrated Services Network. In addition, the concept of a "Relay node" is introduced by the present document.

The present document supports a number of network options. These are summarized in the table 1.

Table 1: Network options

Option	Values	
Support of GFP functionality at transit PINX nodes	Full support	
(subclause 5.2.5)	Partial support	Not applicable in the international network (note 1)
Support of GFP functionality at gateway PINX nodes	Full support	
(subclause 5.2.6)	No support	(note 1)
Continuation of calls with no application association	Supported	(note 2)
(subclause 5.2.6)	Not supported	(note 3)
Relocation of gateway function	Supported	
(subclause 5.2.6)	Not supported	
NOTE 1: Use of these options might result in certain private network supplementary services behaving in an unexpected manner or not working at all. NOTE 2: In this case, VPN calls need to be be routed using a mechanism which can correctly route the call to the terminating access without use of the VPN procedures specified in the present document. NOTE 3: In this case, it is required that the VPN procedures are only used on calls which are routed to addresses which are known to support the VPN application via signalling which supports the APM, otherwise the call will be released.		

2 References

References may be made to:

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

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

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

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

A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

[1] ISO/IEC 11574: "Information technology - Telecommunications and information exchange between systems - Private Integrated Services Network - Circuit-mode 64 kbit/s bearer services - Service description, functional model and information flows".

[2] ISO/IEC 11572: "Information technology - Telecommunications and information exchange between systems - Private Integrated Services Network - Circuit mode bearer services - Inter-exchange signalling procedures and protocol".

[3] ISO/IEC 11582: "Information technology - Telecommunications and information exchange between systems - Private Integrated Services Network - Generic functional protocol for the support of supplementary services - Inter-exchange signalling procedures and protocol".

[4] ISO/IEC 11579-1: "Information technology - Telecommunications and information exchange between systems - Private integrated services network - Part 1: Reference configuration for PISN Exchanges (PINX)".

[5] ISO/IEC 15055: "Information technology - Telecommunications and information exchange between systems - Private Integrated Services Network (PISN) - Specification, functional model and information flows - Transit counter additional network feature".

[6] ETS 300 403-1: "Integrated Services Digital Network (ISDN); Digital Subscriber Signalling System No. one (DSS1); User-network interface layer 3 specification for basic call control; Part 1: Protocol specification [ITU-T Recommendation Q.931 (1993), modified]".

[7] ETS 300 196-1 (1993): "Integrated Services Digital Network (ISDN) - Generic functional protocol for the support of supplementary services - Digital Subscriber Signalling System No. one (DSS1) protocol - Part 1: Protocol specification".

[8] EN 300 356-1 (1997): "Integrated Services Digital Network (ISDN); Signalling System No.7; ISDN User Part (ISUP) version 3 for the international interface; Part 1: Basic services [ITU-T Recommendations Q.761 to Q.764 (1997), modified]".

[9] EN 301 069-1 (1997): "Integrated Services Digital Network (ISDN); Signalling System No.7; ISDN User Part (ISUP); Application Transport Mechanism (APM)".

[10] ETS 300 121 (1992): "Integrated Services Digital Network (ISDN); Application of the ISDN User Part (ISUP) of CCITT Signalling System No.7 for international ISDN interconnections (ISUP version 1)".

[11] ETS 300 899 (work item DE/SPS-01016): "Integrated Services Digital Network (ISDN): Interworking between Signalling System No. 7 ISDN User Part (ISUP) version 2 and Digital Subscriber Signalling System No. one (DSS1) - [ITU-T Recommendation Q.699 modified]".

[12] ETS 300 009 (1991): "Integrated Services Digital Network (ISDN); CCITT Signalling System No.7; Signalling Connection Control Part (SCCP) [connectionless service] to support international interconnection".

[13] ETS 300 134 (1992): "Integrated Services Digital Network (ISDN); CCITT Signalling System No.7; Transaction Capabilities Application Part (TCAP)".

[14] ITU-T Recommendation Q.1400 (1993): "Intelligent Network - Architecture framework for the development of signalling and OA&M protocols using OSI concepts".

[15] CCITT Recommendation X.208 (1988): "Specification of Abstract Syntax Notation One (ASN.1)" (and X.680 containing amendment 1).

3 Definitions and abbreviations

3.1 Definitions

Reference to PINX functionality within the present document refers to "virtual PINX" functionality implemented on the public NNI.

3.2 Abbreviations

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

ACI	Access Control Information
AE	Application Entity
AEI	Application Entity Instance
ALS	Application Layer Structure
ANM	Answer Message
AP	Application Process
APM	Application Transportation Mechanism
APP	Application Transport Parameter
ASE	Application Service Element
ASN1	Abstract Syntax Notation No. one
ATII	Application Transport Instruction Indicators
BGID	Business Group IDentifier
CC	Call Control
COPSS1	Connection-oriented PSS1
CPG	Call Progress Message
DPINX	Destination PINX
DSS1	Digital Subscriber Signalling System No. one
GFP	Generic Functional Protocol
GFT	Generic Functional Transport
GR	Graphical Representation/Rendition
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
LE	Local Exchange
M/O	Mandatory/Optional
MACF	Multiple Association Control Function
MTP-3	Message Transfer Part
NFE	Network Facility Extension
NI	Network Interface
NNI	Network Node Interface
OPINX	Originating PINX
OSI	Open Systems Interconnection
PAN	Public Addressed Node
PIN	Public Initiating Node
PINX	Private Integrated Services Network Exchange
PISN	Private Integrated Services Network
PRI	Pre-Release Information message
PSS1	Private network Q reference point Signalling System No. one
REL	Release message
SACF	Single Association Control Function
SAO	Single Association Object
SCCP	Signalling Connection Control Part
SDL	Specification and Description Language
SID	Signalling Identifier
SSN	Subsystem Number
STP	Signalling Transfer Point
STP	Signalling Transfer Point
TC	Transaction Capabilities
TCAP	Transaction Capabilities Application Part
TE	Transit Exchange
TPINX	Transit PINX
UCEH	Unidentified Context and Error Handling
UNI	User-Network Interface
VPN	Virtual Private Network
VTI	VPN feature Transparency capability Indication

4 Structure of the present document

The description of the ISDN User Part (ISUP) and the TC-user procedures in the present document are structured according to the model described in subclause 5.2. The description is thus divided into two main parts:

- protocol functions;
- non-protocol functions, i.e. exchange nodal functions; this is referred to as the "Application Process".

The present document describes only the part of the total Application Process and Protocol functions in the exchange, that relates to NNI enhancements for the support of private network interconnection, in Virtual Private Network (VPN) application.

The protocol functions are subdivided into two areas; Signalling associations with a bearer (ISUP), and signalling associations without a bearer (connection-oriented TC-user). For calls with a bearer, it describes the use of the services provided by the Application Transportation Mechanism (APM), see EN 301 069-1 [9]. For signalling requiring no bearer, it describes the services provided by Transaction Capabilities Application Part (TCAP).

The signalling association with a bearer is subdivided into three parts: PSS1 Applications Protocol (PSS1 ASE) , Application Transport Mechanism (APM ASE) and ISUP Basic Call (ISUP ASE) These are co-ordinated by the Single Association Co-ordination Function (SACF).

The connection-oriented signalling association without a bearer is subdivided into two parts: Connection-oriented Corporate telecommunications network (COPSS1 ASE), and Transaction Capability (TC ASE). These are co-ordinated by the Single Association Co-ordination Function (SACF).

The Application Process contains all Call Control functions however; the present document will only describe the enhancements required to support VPN applications. The Application Process relevant to private network functionality can be found in other standards (ISO/IEC 11574 [1] and ISO/IEC 11572 [2]), as can that for the public ISUP basic call; see EN 300 356-1 [8].

The service primitive technique, used to define the ASEs and the SACF specific to the application's signalling needs; is a way of describing how the services offered by an ASE or SACF - the provider of (a set) of service(s) - can be accessed by the user of the service(s): the SACF or the Application Process (AP), respectively.

The service primitive interface is a conceptual interface and is not a testable or accessible interface. It is a descriptive tool. The use of service primitives at an interface does not imply any particular implementation of that interface, nor does it imply that an implementation needs to conform to that particular service primitive interface to provide the stated service. All conformance to the ISUP and TC specifications is based on the external behaviour at a node, i.e. on the generation of the correct message structure (as specified in EN 300 356-1 [8])/operation structure (as specified in the present document) and in the proper sequence (as specified in EN 300 356-1 [8] and the present document.)

The structure, and examples of its usage, are illustrated diagramatically in subclause 5.2.

The relationship between the private network functionality and the Application Transport Mechanism services provided by the public NNI is described as a network model in subclause 5.1. The APM ASE provides enhancements to the ISUP capabilities such that the services available to the APM-user (VPN application in this context) for a signalling association requiring a bearer are similar to those offered by TCAP where no bearer is required.

The private network specifications (ISO/IEC 11574 [1]) makes reference to specific private network primitives between Call Control and Protocol Control representing the PSS1 information flows. The Application Process in the present document describes the relationship between these primitives and how they relate to the suitable primitives in the Application Layer Structure (ALS) model for the transport of the PSS1 information flows.

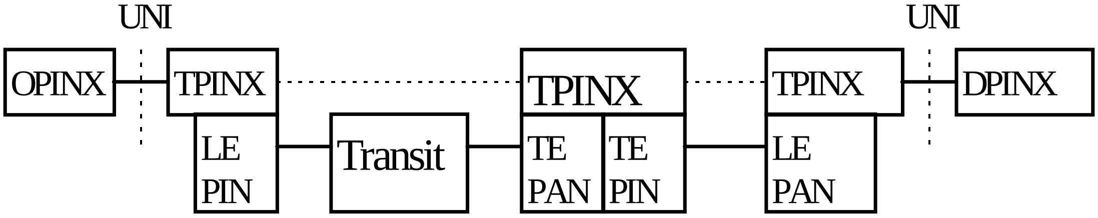
The interworking of User-Network Interface (UNI) protocols and the Network Node Interface (NNI) are provided for informative purposes in annex A (bearer-related) and annex B (bearer unrelated).

Examples of the bearer unrelated signalling mechanism can be found in subclause 10.1.

5 Modelling

The models described in this clause introduce concepts and terminology used in the present document of the VPN application's use of the Application Transport Mechanism (APM) capability for bearer-related signalling and the use of Transaction Capability (TC) for bearer unrelated signalling.

5.1 Network Model



PINX	Private Integrated Services Network Exchange
OPINX	Originating PINX
TPINX	Transit PINX
DPINX	Destination PINX
LE	Local public Exchange
TE	Transit public Exchange
PIN	Public Initiating Node
PAN	Public Addressed Node
Transit	Public Transit node(s)
UNI	User Network Interface

Figure 1: One example of a private network PINX topology and its relationship with the public NNI's PIN/PAN concept

This subclause illustrates the relationship between the VPN and the public network, that provides a service. Figure 1 provides an example of a call from an Originating PINX to a Destination PINX via Transit PINXs. The Transit PINXs in this case are implemented within the public network infrastructure. The public network also provides the service of providing a link between the transit PINXs. In this example, the link is via another public transit node.

The Public Initiating Node (PIN) and Public Addressed Node (PAN) concept is introduced in EN 301 069-1 [9] to assist in the description of the APM. The PIN represents the point in the network where an APM-user, in this case VPN, application for the support of PSS1 information flows entity (PIN) wishes to initiate communications towards a peer APM-user application located at an addressed location (PAN) in the network. A VPN application for the support of PSS1 information flows may result in the establishment of a signalling and bearer association in which case it will use the services of the public basic call.

The PINX functionality requests the services of the public network in order to establish a signalling associating with the subsequent PINX in the virtual private network. The initiating PINX application supplies a normal public E.164 number which is used to route through the public network thus establishing an association between the PIN and the PAN. The PAN identifies the particular APM-user application by the Context Identifier value carried within the Application Transport Parameter, in this case "PSS1 ASE (VPN)". The PAN identifies the particular PINX application related to a specific corporate network identified by a business group identity (e.g. Business Group Identity (BGID) parameter).

The nature of the PINX functionality (i.e. Originating PINX, Destination PINX, Transit PINX or Gateway PINX) is independent of the mechanism described here, and is solely dependant on the topology of the virtual private network.

The public basic call mechanism is employed to provide an association between the PIN and the PAN. In routeing through the public network, the call may pass through intermediate public nodes with or without the ability to support the private functionality. However as the private application is not addressed by the particular call instance, it will behave as a normal intermediate public node.

Figure 2 illustrates an example of a public message sequence for a call requiring a bearer (ISUP) in the scenario of figure 1. Figure 3 illustrates the public operation sequence (TC) for a call not requiring a bearer.

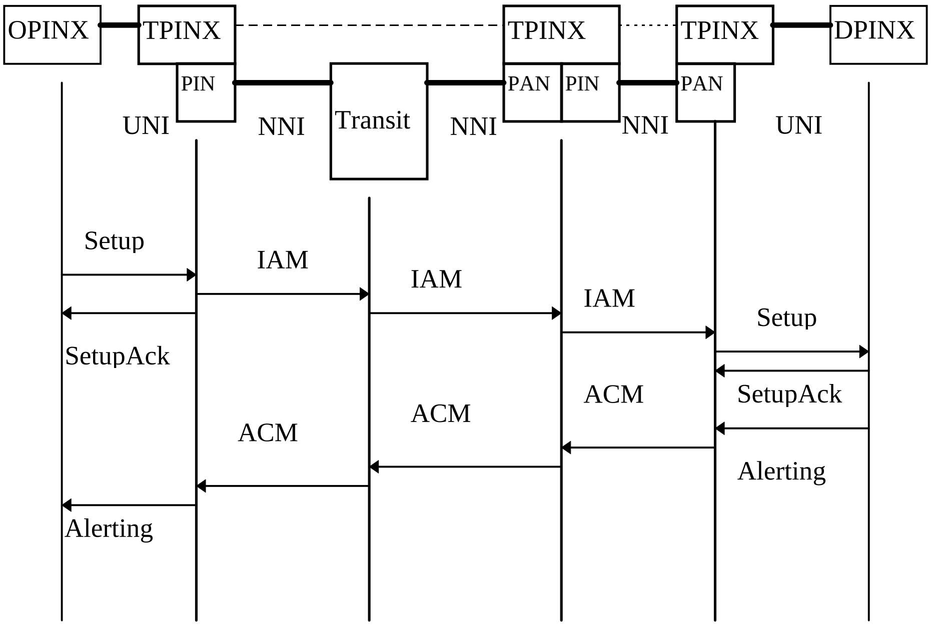


Figure 2: One example of a message sequence for call with bearer

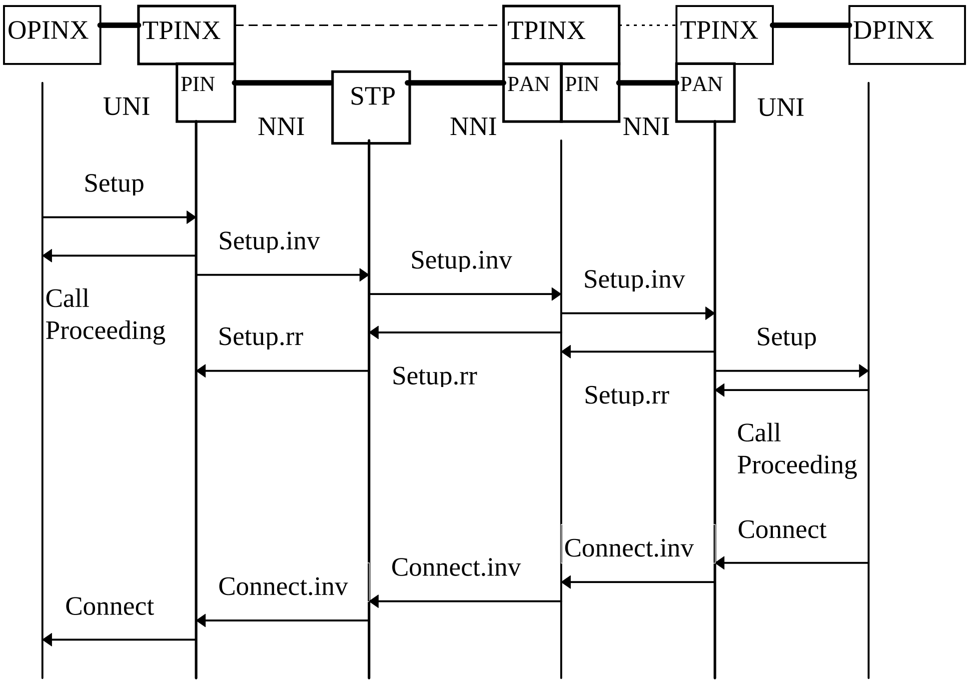


Figure 3: One example of an operation sequence for call without a bearer

5.2 Specification model

5.2.1 Introduction

The model used to structure the description of ISUP and TC-user application procedures is based on the Open Systems Interconnection (OSI) Application Layer Structure (ALS) model (see ITU-T Recommendation Q.1400 [14]). This subclause presents the model and gives a general description of its operation. This subclause shows the generalized model for the "Exchange Application Process" for the support of PSS1 information flows in virtual private networks, VPN application for the support of PSS1 information flows over the public Network Nodal Interface (NNI). It shows how the application makes use of the Application Transportation Mechanism (APM) which is described in detail in EN 301 069-1 [9].

5.2.2 General model

The generalized model for the bearer-related (ISUP)/bearer unrelated (TC) VPN Application Process is shown in figure 4. This figure does not represent the situation at any specific point during ISUP/TC procedures, but instead it shows the full picture of the architecture. The specific application of this model is discussed in subclause 5.2.3. Figure 4 shows the primitive interfaces between the functional blocks, as used in the body of the present document for calls with a bearer (ISUP)/without a bearer (TC).

The definition of the interfaces a to k are:

a) Interface between the Application Process (AP) nodal functions and the SACF for the support of PSS1 information flows in VPN applications over the NNI: see subclause 6.2.2.

b) Interface to PSS1 ASE which defines the protocol control procedures and the formats and codes in the APP for the support of PSS1 information flows in VPN applications: see subclause 9.1.

c) Interface between SACF and UCEH ASE representing the handling of unidentified context identifier values and error cases associated with the Application Transport mechanism: EN 301 069-1 [9].

d) Interface between SACF and APM ASE representing enhancements of the public (ISUP) functionality for providing a transportation mechanism for the support of various applications (APM-user) over the NNI: (this interface is beyond the scope of the present document): EN 301 069-1 [9].

e) Interface to public ISUP basic call signalling ASE: (this interface is beyond the scope of the present document) EN 301 069-1 [9].

f) Interface between SACF and NI function: (this interface is beyond the scope of the present document) EN 301 069-1 [9].

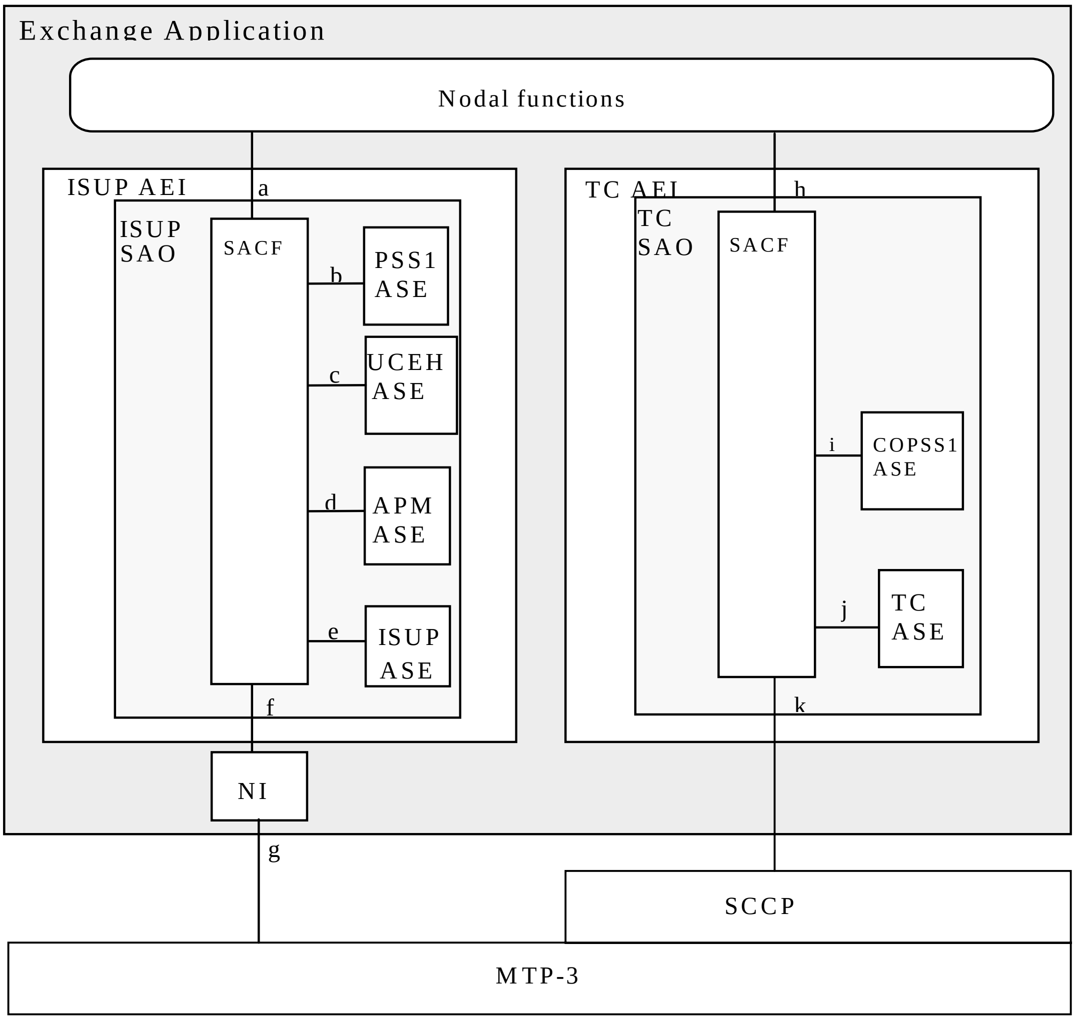
g) Interface to MTP-3: (this interface is beyond the scope of the present document) EN 301 069-1 [9].

h) Interface between TC SACF and AP: see subclause 6.3.2.

i) Interface between TC SACF and COPSS1 ASE which performs the function of protocol control for bearer unrelated connection-oriented signalling: see subclause 10.2.

j) Interface between TC SACF and TC ASE which provides the services defined in ETS 300 134 [13]: see subclause 11.1.

k) Interface between TC SACF and SCCP which provides the services defined in ETS 300 009 [12]: see subclause 12.1.



Abbreviations:

AEI	Application Entity Invocation
ASE	Application Service Element
APM	Application Transportation Mechanism
APM-user	Application Transportation Mechanism user application
ISUP	ISDN User Part
MTP	Message Transfer Part
NI	Network Interface
PSS1	Private network Q reference point Signalling System No. one
SACF	Single Association Control Function
SAO	Single Association Object
UCEH	Unidentified Context and Error Handling

Figure 4: ISUP and Connection-oriented signalling specification model

With respect to figure 4, all functions also have an interface to a "management application"; this is not defined as a formal primitive interface.

The term "Exchange Application Process" is used to describe all the application functionality in an exchange. ISUP is a part of the Exchange Application Process. Thus the ISUP nodal functions shown on the model are referred to as the ISUP Application Process functions in the body of the present document. Similarly, the bearer unrelated Transaction Capability nodal functions shown on the model are referred to as the TC Application Process functions in the body of the present document.

The ISUP/TC AEI provides all the communication capabilities required by the ISUP/TC Nodal functions. For simplicity a ISUP/TC Application Entity Instance (AEI) is defined as containing just one SAO; this avoids the need to specify a Multiple Association Control Function (MACF). Thus all co-ordination of ISUP signalling associations is performed via the ISUP Nodal functions. Similarly, the co-ordination of the TC signalling associations is performed via the TC nodal functions.

The SACF has the responsibility of co-ordinating the flow of primitives between its interfaces in the appropriate manner.

The ISUP ASE is defined in EN 300 356-1 [8]. Its main responsibilities are basic call procedures and the handling of protocol errors and unrecognized information. The monolithic nature of EN 300 356-1 [8] means that both Public Call Control and Protocol Control functionality are defined together. It is not the intention of the present document to re-define EN 300 356-1 [8] in ALS format; therefore it is referenced en-bloc within the present document as the ISUP ASE. Conceptually, this should be considered to represent a logical division between the protocol control functionality within the ISUP ASE and its associated call control functionality within the application process. The modelling and interfaces with respect to this are beyond the scope of the present document (see EN 301 069-1 [9]).

The APM ASE provides the means for the transfer of information between nodes for signalling requiring a bearer, and to provide generic services to applications, while being independent of any of these. It is responsible for the enhancements to the NNI (ISUP) for the support of a mechanism which allows various applications to transport their information flows via the NNI. Its main responsibility is to provide message segmentation/reassembly in order to provide the APM-user the ability to transport up to 2 048 octets of application information. The APM ASE is able to support multiple APM-users where each is treated independently and is provided with the same level of service. It consists of two distinct sets of functions; one set used as the PAN and one set used as the PIN (supporting the signalling association towards the PAN). The PIN/PAN concept is explained in subclause 5.1 of EN 301 069-1 [9].

The UCEH ASE provides a compatibility mechanism for the case where various levels of application (context) support exists within network nodes as well as APM reassembly error handling. The UCEH ASE is responsible for the procedures related to the reception of an Application Transport parameter referencing an unidentified context identifier and the corresponding handling of a notification that a particular context identifier is not supported at a remote node. (see EN 301 069-1 [9]) It is also responsible for the handling of APM reassembly error cases.

The PSS1 ASE is a user of the services offered by the APM ASE. It is responsible for preparing the private signalling information in a form that can be transported by the public application transportation mechanism (APM).

The TC ASE provides the means for the transfer of information between nodes for signalling without a bearer, and provides generic services to applications, while being independent of any of these. The TC ASE is defined in ETS 300 134 [13].

The COPSS1 ASE is a user of the services offered by the TC ASE. It consists of two distinct sets of functions related to the PAN and PIN of connection-oriented bearer unrelated signalling (TC dialogue).

To handle any particular ISUP/TC function the Exchange Application Process creates an instance of the required ISUP/TC nodal functions. The AP will create instances, as required, of the ISUP/TC AEI. The Network Interface (NI) function exists to distribute messages received from the Message Transfer Part (MTP-3) to the appropriate instance of the ISUP AEI. There is only one instance of the NI in an exchange. Messages are distributed to the appropriate TC AEI based on the Subsystem Number (SSN) and the TC dialogue identity.

The SCCP interface is described in ETS 300 009 [12].

The SAO contained in the ISUP AE is one of the following types:

a) Public Initiating Node

   This contains:

   - Outgoing ISUP ASE, Initiating APM ASE, Initiating UCEH ASE, Outgoing PSS1 ASE and ISUP SACF.

b) Public Addressed Node

   This contains:

   - Incoming ISUP ASE, Addressed APM ASE, Addressed UCEH ASE, Incoming PSS1 ASE and ISUP SACF.

The SAO contained in the TC AE for connection-oriented bearer unrelated signalling is one of the following types:

a) Public Initiating Node

This contains:

- Outgoing COPSS1 ASE, TC ASE and TC SACF.

b) Public Addressed Node

This contains:

- Incoming COPSS1 ASE, TC ASE and TC SACF.

5.2.3 Dynamic primitive flows

5.2.3.1 Bearer-related signalling flows

Figures 5 and 6 illustrates the dynamic primitive flows for a VPN call with PSS1 information flow support being supported over the NNI (ISUP) for the case where a call control message is coincident with the application information flow. Figure 5 shows the case when a message is being sent, figure 6 shows the case when a message is being received.

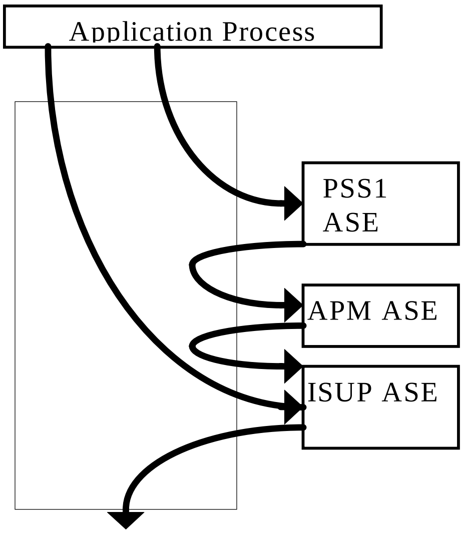


Figure 5: Coincident CC message; AP sending

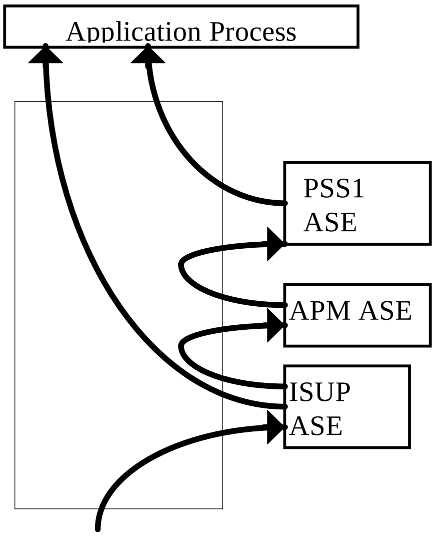


Figure 6: Coincident CC message; AP receiving

Figure 7 and 8 illustrate the dynamic primitive flows for the NNI support of the PSS1 information flow in a VPN call where no call control messages are sent coincidently. That is, the APM ASE initiates a primitive towards the ISUP ASE which in turn sends an APM message which will provide a mechanism for supporting the information flow.

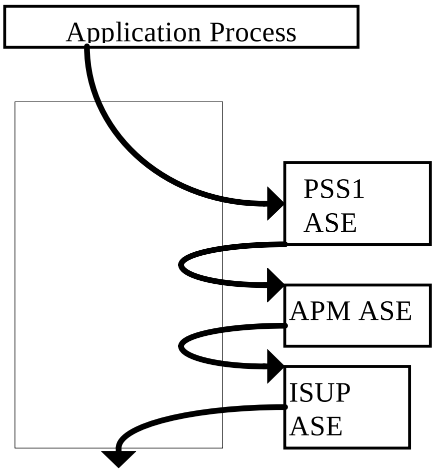


Figure 7: No coincident CC message; AP sending

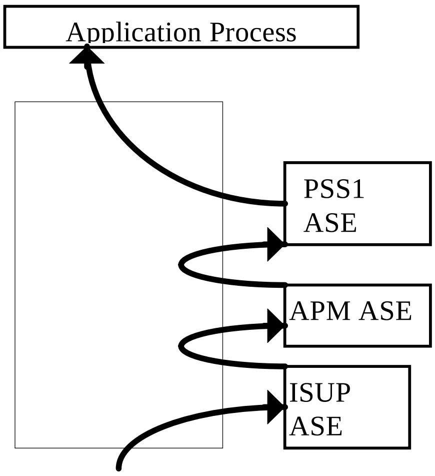


Figure 8:No Coincident CC message; AP receiving

5.2.3.2 Bearer unrelated signalling flows

Figure 9 and 10 illustrate the dynamic primitive flows for a VPN signalling connection without a bearer being supported over the NNI (TC).

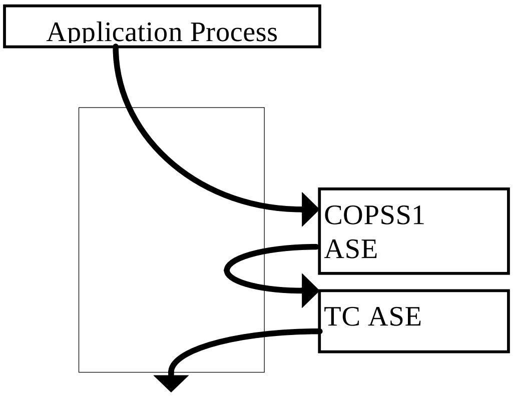


Figure 9: Bearer unrelated; AP sending

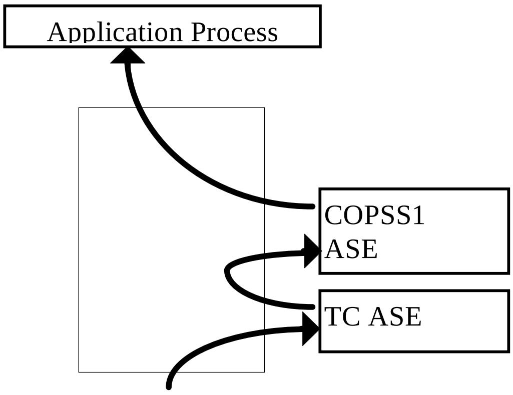


Figure 10: Bearer unrelated; AP receiving

5.2.4 Basic Call

The public network can be considered as a virtual Transit PINX in the establishment of VPN calls requesting support of PSS1 information continuity, thus meeting the functional requirements defined in PSS1 basic call for a Transit PINX.

In case a fallback situation occurs inside the VPN (i.e. a loss of PSS1 information flows continuity), the public network provides Gateway PINX functionality, similarly to the behaviour of a Gateway PINX inside a private network interconnecting PINX to a public network.

5.2.5 Transit PINX function - Generic Functional Protocol (GPF)

Two cases can be distinguished to describe the public network behaviours for VPN calls or bearer unrelated VPN signalling connections supporting the functional continuity of PSS1-GF procedures (i.e. PSS1 Generic functional protocol for the support of private network supplementary services):

1) full support of GFP functionality: the VPN provides full Transit PINX functionality as defined in PSS1-GF (ISO/IEC 11582 [3]), which includes analysis of the Network Facility Extension (NFE) field of the received Facility information elements;

2) partial support of GFP functionality: the VPN node performs the same functions as in option 1 except for the handling of the Facility information element with the protocol profile set to "networking extensions". The following summarizes the handling of the Facility information element:

   - The VPN would pass on PSS1-GF information received in a Facility information element transparently between two PINXs that are directly connected to the VPN.

   - The VPN would not look at Facility IE contents, in particular the NFE, to determine for whom the Facility information element was intended.

The use of option 2 in a network may result in the incorrect operation of some network services. In order to avoid this problem, it is necessary to take into account a network topology so that such a node is not used in conjunction with such services.

Across the international interface, option 1 capability has to be used and supported and the use of option 2 may be agreed to be supported across the interface between public networks through bilateral agreements between network operators.

5.2.6 Gateway PINX function

The Gateway PINX (GPINX) functionality is invoked when it is determined that the continuity of PSS1 information flows cannot be maintained. The GPINX can be invoked as a result of analysis where it is determined that the destination does not support PSS1 information flows (note), or through an indication that the intermediate network signalling does not support the transport of the PSS1 information flows, or through an indication that the APM or APM-user is not supported in the PAN (see subclause 6.2.3.2.5).

NOTE: This includes the situation where the PAN is the destination local exchange acting as a Transit PINX with an outgoing access which supports PSS1 information flows but the call is released by the PAN before sending the call establishment request to the outgoing access.

Where it is determined that the PSS1 information flow continuity cannot be maintained, there are two options:

1) allow the call to continue (choose to perform the gateway function or request that it be performed elsewhere);

2) release the call.
   If the call is allowed to continue, it is necessary that the public basic call information used to route the VPN call is sufficient to allow the call to proceed and terminate successfully. The use of these options is a network operator's choice based on the level of service being offered to the private network owner.

The support of the Generic Functional Protocol (GFP) as part of the Gateway PINX functionality is optional according to ISO/IEC 11582 [3]. It is therefore a network operator's option to support the Generic Functional Protocol handling procedures. It should be noted that some services may behave in a less than desirable manner if the GFP is not supported.

In order to reduce the effect of network signalling load resulting from the support of the PSS1 information flows in the VPN, it is a network operator's option to support the mechanism for moving the GPINX functionality as close as possible to the originating end of the call path. There are three possibilities:

a) Gateway PINX function provided at point of "break-out"

   This is when the Gateway PINX function is performed at the point in the network where it is determined that the gateway is required.

b) Gateway PINX function provided by cooperation between nodes (movement of the gateway functionality to an earlier point in the call path)

   This is when the node that determines that a gateway PINX function is required performs the "basic call" gateway function (and the GF gateway function if it supports it) for the IAM message. If that node was informed that a previous node is capable of providing the gateway functionality (Gateway transformation capability indication received in the IAM, sent by an earlier node in the call path), then it sends a request backwards to do so. When the node with the capability to transform into a gateway PINX receives the request, it then performs the gateway functionality (basic call and GF, if supported) from that time onwards for that call.

6 Application Process functions

6.1 General

The modelling of the Application Process (AP) is beyond the scope of the present document, however, in order to appreciate the role of the AP for the purposes of the present document, it can be considered to consist of three different types of functionality that are relevant to the support of private networks over the public network nodal interface. These are, Public network Application Transport Mechanism (as defined in EN 301 069-1 [9] and ISUP basic call, see EN 300 356-1 [8]; and the VPN applications for the support of PSS1 functionality, as defined in the present document.

The aspect of the application process that the present document introduces is the required co-ordination between the public network and VPN (for the support of PSS1 information flows) application process functionality in order to provide the appropriate transportation of PSS1 information flow via:

- the combination of public ISUP basic call and the Application Transport Mechanisms;
- using transaction capability mechanisms.

The private network functionality being provided by the VPN is described in subclause 5.2.4, 5.2.5 and 5.2.6. In order to show the relationship between the VPN AP and the PSS1 Call Control logic, the present document defines the mapping between the Call Control/Protocol Control, see ISO/IEC 11572 [2] and the SACF interface (a). It also describes the additional VPN specific procedures. The description of either the public or PINX application processes are beyond the scope of the present document.

The definition of the primitive interface at the application process/SACF for the public Application Transport Mechanism is beyond the scope of the present document.

6.2 VPN Application Process functions - Connection with Call (Bearer-related)

6.2.1 Introduction

The function of the Public NNI support of VPN applications aspect of the Application Process (AP) is to co-ordinate between the private network (PSS1) application process and the public application process functionality. When the private application requires the establishment a signalling association with a bearer, the AP converts the private address information into the form that the public application process can use for routeing the call from the PIN to the appropriate exchange in the public network, Public Addressed Node (PAN), which contains the adjacent PINX functionality. The PIN/PAN concept is described in EN 301 069-1 [9]. The specific private network use of the concept is described in subclause 5.1 of the present document. Details of the public basic call routeing information requirements can be found in EN 300 356-1 [8]. The conversion of private information to a form suitable for routeing through the public network is beyond the scope of the present document. It is network specific as to how the appropriate public routeing information is generated (e.g. it may be a result of local analysis, or IN mechanisms may be employed).

It is not the intention of the present document to re-define the PSS1 PINX functionality, therefore the call control defined in ISO/IEC 11574 [1] applies. The purpose of the present document is to describe how, together with the ISUP basic call and APM, the services expected by PSS1 at the Call Control (CC)/Protocol Control (PC) interface (defined in ISO/IEC 11572 [2]) are fulfilled in a VPN, thus achieving PSS1 information flow continuity over the public NNI.

The PSS1 primitive interface between Call Control and Protocol Control (see ISO model in ISO/IEC 11572 [2]) and that between Generic Functional Transport (GFT) - Control and Protocol Control (see ISO model in ISO/IEC 11582 [3]) are not seen on any interface in the ALS. It is not the intention of the present document to model the AP, however to illustrate the relationship between the present document and the PINX functionality defined by ISO standards, figure 11 can be used. The relevancy of the PSS1-Call Control and PSS1-GFP shown in figure 11 is dependant upon the PINX functionality being provided by a node.

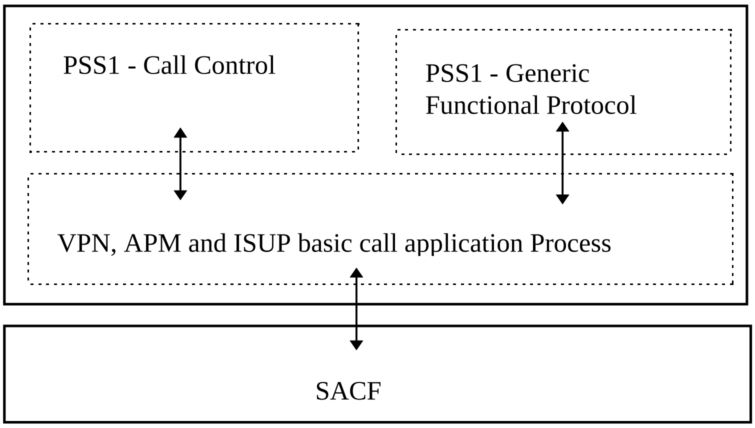

PSS1 - Call Control
PSS1 - Generic Functional Protocol
VPN, APM and ISUP basic call application Process
SACF

Figure 11: Relationship between PSS1 primitive interfaces and ALS model

In order for the PSS1 information flow continuity to be maintained in a virtual private network, it is necessary to introduce additional procedures that allow VPNs to co-exist in the public network and to handle scenarios that are specific to the support of these over the public network. These procedures include the possible use of a Business Group Identifier (BGID) to uniquely identify a corporate network, the transfer of VPN identities, and the appropriate setting of Application Transport Instruction Indicators (ATII) in order to cater for error cases.

At call establishment the PINX functionality located at the PAN will determine that additional private digits may need to be received (overlap sending of private digits). In this case it is necessary for the PAN to send back towards the PIN a "setup acknowledgement" indication in order to confirm the signalling association through the network such that the PIN can reliably send additional digits towards the PAN.

In order for the VPN calls requesting PSS1 information flows support to operate correctly, it is necessary that the signalling capability of intermediate public nodes between the PIN and PAN are able to transport the AP Protocol (APP). If the subsequent link(s) does not support the APM and hence the transport of the VPN information is lost, or if the addressed node does not have the APM or PINX functionality, then the node shall invoke the Gateway PINX functionality described in subclause 5.2.6. This signalling capability may not be fulfilled if the call is routed through nodes such as an ISUP version 1 node (ETS 300 121 [10]), a public gateway node or a non-ISUP node. To cater for the case where the intermediate nodes and their associated signalling capabilities cannot support the transport of PSS1 information flows using the ATM, or the case when the call addresses a node without the APM or without the PSS1 PINX functionality and is allowed to continue (network option), it is necessary to have a mechanism to confirm that the VPN call supports PSS1 information flows ("VPN feature transparency capability" indication (VTI)) and to inform the preceding PINX that Gateway PINX functionality is required to be invoked. The mechanism to have the Gateway function invoked needs to work in an implicit manner by invoking the GPINX functionality:

- on the non-reception of a positive confirmation that PSS1 information flow continuity is supported ("VPN feature transparency capability" (VTI) indication);
- on reception of a notification "unidentified context";
- on reception of a confusion message with a diagnostic field indicating that the Application Transport parameter has been discarded.

The node shall make a decision whether to release the call immediately or to allow it to continue (network operator's option based on the level of service being offered to the private network owner). If the call is allowed to continue, then it is necessary that the public basic call information is sufficient to allow the call to be terminated successfully.

When it is determined that Gateway PINX functionality has to be invoked, the "node determining gateway PINX functionality is required" may (as a network option) request a PINX located closer to the originating end of the call, "node capable of gateway PINX transformation", to perform the Gateway function thereby reducing the signalling load on the public network resulting from the private network signalling. A mechanism has been introduced to allow this transformation of an earlier Originating PINX or Transit PINX in the call path to an Outgoing Gateway PINX. The mechanism relies on the node sending forward an indication that it is able to perform the transformation and a subsequent node, on determining that a Gateway function is required, sending backwards a request to transform into a gateway PINX.

6.2.2 Primitive interface (AP - ISUP SACF)

The primitive interface (interface (a) in figure 4) between the AP and the ISUP SACF consists of primitives required to support the public network basic call functionality, and those to support the VPN functionality. The primitives related to the public network functionality are beyond the scope of the present document although references are made to them through functional inferences within the text. The public basic call specification is not described using ALS concepts, hence the need for functional inferences to the public basic call functionality rather than specific references to primitives. The primitives related to the VPN functionality are described in the present document.

Table 2: Primitives between AP and ISUP SACF (Virtual Private Network Support)

Primitive name	Types
PSS1_Data	Indication/Request
PSS1_Error	Indication
Remote_Status	Indication

6.2.3 Procedures

6.2.3.1 PSS1 Information Flows

The private network service descriptions are defined by ISO in the series of International Standards describing the Private Integrated Services Network. These services are built upon the Circuit-mode 64 kbit/s bearer services standard (ISO/IEC 11574 [1] and ISO/IEC 11572 [2]), and the Generic functional protocol for the support of supplementary services standard (ISO/IEC 11582 [3]). The support of the private network services in a virtual private network is achieved through the transport of the necessary information flows over the public network signalling between entities that support the private network service descriptions. Tables 3, 4 and 5 describe how the PSS1 information flows are distributed across primitives on the AP/SACF interface.

Table 3: Mapping between PSS1 primitives defined in ISO/IEC 11572 [2] and AP/ISUP SACF primitives

Primitives to/from CC Interface (ISO/IEC 11572 [2])			ISUP Messages	Primitives to/from AP/SACF Interface (PSS1 ASE)
PC_SETUP	REQ	→	IAM	+ PSS1_DATA.Req
	IND	←	IAM	+ PSS1_DATA.Ind
	RES	→	ANM/CON	+ PSS1_DATA.Req
	CONF	←	ANM/CON	+ PSS1_DATA.Ind
PC_MORE_	REQ	→	APM/ACM	+ PSS1_DATA.Req
INFORMATION	IND	←	APM/ACM/CPG	+ PSS1_DATA.Ind
PC_INFORMATION	REQ	→	APM	+ PSS1_DATA.Req
	IND	←	APM	+ PSS1_DATA.Ind*1
PC_PROCEED	REQ	→	ACM/CPG	+ PSS1_DATA.Req
	IND	←	ACM/CPG	+ PSS1_DATA.Ind
PC_ALERTING	REQ	→	ACM/CPG	+ PSS1_DATA.Req
	IND	←	ACM/CPG	+ PSS1_DATA.Ind
PC_PROGRESS	REQ	→	ACM/CPG	+ PSS1_DATA.Req
	IND	←	ACM/CPG	+ PSS1_DATA.Ind
PC_REJECT	REQ	→	PRI/REL	+ PSS1_DATA.Req (PRI only)
	IND	←	PRI/REL	+ PSS1_DATA.Ind (PRI only)
PC_DISCONNECT	REQ	→	PRI/REL	+ PSS1_DATA.Req (PRI only)
	IND	←	PRI/REL	+ PSS1_DATA.Ind (PRI only)
PC_RELEASE	REQ	→	PRI/REL	+ PSS1_DATA.Req (PRI only)
	IND	←	PRI/REL	+ PSS1_DATA.Ind (PRI only)
DL_RESET	IND	←	n/a	

Table 4: Mapping between PSS1 primitives defined in ISO/IEC 15055 [5] and AP/ISUP SACF primitives

Primitives to/from CC Interface (ISO/IEC 15055 [5])			ISUP Messages	Primitives to/from AP/SACF Interface (PSS1 ASE)
PC_TRANSIT_COUNTER	REQ	→	IAM	+ PSS1_DATA.Req
	IND	←	IAM	+ PSS1_DATA.Ind

Table 5: Mapping between PSS1 primitives defined in ISO/IEC 11582 [3] and AP/ISUP SACF primitives

Primitives to/from CC Interface (ISO/IEC 11582 [3])			ISUP Messages	Primitives to/from AP/SACF Interface (PSS1 ASE)
PC_DATA	REQ	→	APM	+ PSS1_DATA.Req
	IND	←	APM	+ PSS1_DATA.Ind
PC_NOTIFY	REQ	→	IAM/ACM/ANM/CON/CPG/PRI/APM	+ PSS1_DATA.Req
	IND	←	IAM/ACM/ANM/CON/CPG/PRI/APM	+ PSS1_DATA.Ind

6.2.3.2 NNI indications and procedures

In order to support the PSS1 information flows across the public network, it is necessary to introduce additional procedures and information flows to allow the virtual private network to co-exist in the public network environment.

6.2.3.2.1 Handling of address information

Procedures at the PIN

The called party number sent in the PSS1_Data request primitive sent at call establishment shall also be transferred in the ISUP generic number parameter with the Number qualifier indicator coded "additional called party number" in the IAM message.

The calling party number sent in the PSS1_Data request primitive sent at call establishment is also transferred in the ISUP generic number parameter with the Number qualifier indicator coded "additional calling party number" without taking into account the public CLIR and CLIP supplementary services.

The connected number received in the PSS1_Data indication primitive received in conjunction with the primitive corresponding to the CON or ANM message and the connected subaddress received according to the public basic call procedures shall be transferred to the access signalling system without taking into account the public COLP and COLR supplementary services.

Procedures at the PAN

The calling party number received in the PSS1_Data indication primitive received in conjunction with the IAM message and the calling party subaddress received according to the public basic call procedures shall be transferred to the access signalling system without taking into account any possible public CLIP and CLIR supplementary service.

The connected number sent in the PSS1_Data request primitive sent in conjunction with the primitive corresponding to the CON or ANM message shall also be transferred in the ISUP generic number parameter with the Number qualifier indicator coded "additional connected number" without taking into account the public COLP and COLR supplementary services in the primitive corresponding to the CON or ANM message.

The connected subaddress shall be transferred according to the public basic call procedures without taking into account the public COLP and COLR supplementary services.

6.2.3.2.2 Business Group Identifier

The business group identifier is either supplied over the incoming user-network interface (UNI) access, or it has an implicit value tied to the incoming access. The BGID is only required for call establishment (IAM message (ISUP)) and is mandatory over the international interface and has global significance. It is an operator's network option to employ an alternative mechanism for identifying a business group within its own domain. On receipt of a business group identifier that is not recognized by the PAN, the call shall be released with cause 63 (service or option not available - unspecified) and the management function notified.

6.2.3.2.3 Application Transport Instruction Indicators

The ATII are required to be sent in conjunction with any private network specific information in order to handle error cases such as an unidentified context at the PAN or reassembly errors. They are to be set according to the particular needs of the application. That is, if the requested functionality is essential to the call, then the ATII should be set to release call. Alternatively if actions are required to be performed to gracefully handle the case where the communication is not successful but the call is to continue, a notification should be requested. If there is no real need to indicate an unsuccessful communication with the PAN, then no actions need to be requested in the ATII.

6.2.3.2.4 Acknowledgement from peer application (Overlap sending)

Procedures at the PAN

On reception of the PC_More_Information.Request primitive, the AP shall send a PSS1_Data.request primitive indicating "Setup Acknowledgement" in conjunction with the primitive corresponding to a suitable first backwards ISUP message (ACM, or APM) to be sent towards the PIN.

Procedures at the PIN

On reception of the PSS1_Data.indication primitive indicating "Setup Acknowledgement", the AP shall send PC_More_Information.Indication primitive.

6.2.3.2.5 Subsequent node does not support APM/VPN

Procedures at the PAN

When a call is being established with PSS1 feature transparency capability, shall it implicitly request this capability by the presence of the APP parameter with Application Context Identifier coded "PSS1 ASE (VPN)" in the IAM message. If the PAN determines that the VPN call supports PSS1 information flows continuity, the PAN shall include in the first backwards message the "Call with VPN feature transparency capability"(VTI) indication in an APP parameter.

Procedures at the PIN

On reception of the "Call with VPN feature transparency capability (VTI)" indication at the PIN in an ACM, CPG, CON, ANM, PRI or APM message, the PIN shall apply the procedures defined for VPN calls with PSS1 information flows continuity. After the sending of an IAM, the PIN shall not send APP parameters (containing Facility "Networking extensions" information elements or notifications) before receipt of the "Call with VPN feature transparency capability" (VTI) indication. Such information may be discarded.

If the option to continue calls with no application association is supported, then the Gateway PINX functionality shall be invoked in the following cases. The gateway PINX is described in subclause 5.2.6:

- in the case where ISUP receives a Confusion message containing a cause parameter non-existent or not implemented, discarded (99) with diagnostics indicating the APP, then the APM is not supported in the subsequent node;
- on reception of a notification that the peer APM user was not present at the PAN (APP parameter with Access Control Information (ACI) field coded "Unidentified Context and Error Handling (UCEH) ASE" and with the Application Transport Notification information coded "PSS1 ASE (VPN)", received in an ACM, CON, ANM, CPG, APM or PRI message);
- on receipt of the primitive corresponding to the CON message without the indication of "call with VPN feature transparency capability";
- on receipt of the primitive corresponding to the ANM message without the indication of "call with VPN feature transparency capability" if the indication has not been received in a previous message;
- on receipt of the primitive corresponding to the REL message if the "call with VPN feature transparency capability" indication has not been received in a previous message.

Whereas the loss of PSS1 information flows continuity cannot be determined on receipt of an ACM without a "call with VPN feature transparency capability" indication, receipt of a CON/ANM/REL without any indication when no indication has previously been received shall be considered to be an implicit confirmation that the call does not support PSS1 information flows.

If the option to continue calls with no application association is not supported, then, on the receipt of the above indications that the call does not support the PSS1 information flows continuity, then the call shall be released and the management function notified.

6.2.3.2.6 Gateway PINX transformation request mechanism (network option)

It should be noted that the use of this mechanism has the effect of removing intermediate transit PINXs between the "node capable of gateway PINX transformation" and the "node determining gateway PINX functionality is required"; therefore the network topology needs to be taken into account when using this feature.

Receipt of the "Gateway PINX Transformation Request" indication takes precedence over the procedures described in subclause 6.2.3.2.5 which may be invoked on reception of the "VPN feature transparency capability (VTI)" indication.

Node capable of gateway PINX transformation

A node with PINX functionality that has the capability of transforming from either an Originating PINX or Transit PINX into a Gateway PINX ("node capable of gateway PINX transformation"), shall indicate "PINX with gateway transformation capability" in the forward direction in the initial setup message.

On receiving a "Gateway PINX transformation request" indication in an ACM, CPG, CON, ANM, PRI or APM message, a node shall check the note in memory to determine if a previous node has the capability of transforming into a Gateway PINX. If not, then the node shall transform its PINX functionality to behave as an Outgoing Gateway PINX for all subsequent private network specific information received. Procedures as described in subclause 6.2.3.2.5 for the PAN when the Gateway PINX function is invoked shall apply, in particular the sending in the backwards direction of the "Call with VPN feature transparency capability (VTI)" indication if not already sent.

Intermediate node

Any node with PINX functionality subsequent to the "node capable of gateway PINX transformation" shall make a note in memory that a previous node has the capability and also indicate the same in the forward direction.

On receiving a "Gateway PINX transformation request" indication, a node shall check the note in memory to determine if a previous node has the capability of transforming into a Gateway PINX. If so, then the request shall be passed unchanged.

The node shall continue as a Transit PINX for any subsequent PSS1 information received. Such information may continue to be received until the Gateway PINX transformation request has been processed by the "node capable of gateway PINX transformation".

Node determining gateway PINX functionality is required

A node with PINX functionality that determines that an Outgoing gateway PINX functionality must be invoked ("node determining gateway PINX functionality is required") shall perform the appropriate actions on the private network specific information received as defined by ISO (see subclause 5.2.6).

It may then, as a network option, check the note in memory to determine if a previous node has the capability of transforming into a Gateway PINX. If the capability is available, the node shall indicate "Gateway PINX transformation request" in the backwards direction and shall send the "VPN feature transparency capability (VTI)" indication set to "no indication".

The node shall continue as a Gateway PINX for any subsequent PSS1 information received. Such information may continue to be received until the Gateway PINX transformation request has been processed by the "node capable of gateway PINX transformation".

6.2.3.3 Relay Node

The Relay node functionality distinguishes VPN calls, and shall relay such calls to designated PINX functionality emulated by the public network equipment, or to a designated physical PINX. This may be via other Relay node functionality which includes transparent handling of private networking information.

A Relay node allows a network to provide PINX functionality remotely from a UNI access. A relay node does not have PINX functionality, rather it provides a transparent link between an access and the node containing the PINX functionality within the network.

When the relay node requires the establishment of a signalling association with a bearer, the AP shall generate public routeing information in the form that the public application process can use for routeing the call from the PIN to the appropriate exchange in the public network, PAN, which contains the PINX functionality. Details of the Public basic call routeing information requirements can be found in EN 300 356-1 [8]. The public routeing information is implicitly tied to the particular business group identifier associated with the access.

The private network specific information shall be passed transparently and distributed to primitives on the AP/ISUP SACF interface in the same manner as if the information had been received from the private call control logic, hence private network specific information flow transparency is achieved.

6.2.4 Exceptional procedures

6.2.4.1 Signalling congestion

In order to avoid signalling link congestion in the No.7 network, it is necessary that applications that contribute signalling load towards a congested link limit such signalling in a controlled manner. On receipt of a congestion indication (in a Remote_Status.indication primitive) the application shall reduce signalling traffic load in several steps. The following procedure is applicable on a destination basis.

When the first congestion indication is received, the signalling traffic load shall be reduced by one step. At the same time two timers T-C1 and T-C2 are started. During T-C1 all received congestion indications shall be ignored in order not to reduce traffic too rapidly. Reception of a congestion indication after the expiry of T-C1, but still during T-C2, shall decrease the signalling load by one more step and restart T-C1 and T-C2. This step-wise reduction of the application signalling load shall be continued until maximum reduction is obtained by arriving at the last step. If T-C2 expires (i.e. no congestion indications having been received during the T-C2 period), signalling load shall be increased by one step and T-C2 shall be restarted unless full signalling load has been resumed.

Timers T-C1 and T-C2 have the following recommended range:

T-C1 = 300-600 ms;

T-C2 = 5-10 s.

The number of steps of traffic reduction and the type and/or amount of increase/decrease of traffic load at the various steps are considered to be an implementation matter. The steps change with respect to the timers and the reception of the Remote_Status primitive indicating "signalling congestion".

The two timer method, as described above, would allow for a smooth reduction and resumption of signalling towards the MTP in the case of congestion. The use of different timer values for different applications would allow for a mechanism of prioritization of the applications. These timer values should be definable by the operator.

6.2.5 Error indication primitive

On reception of a PSS1_Error primitive containing an error notification indicating "unidentified context", if the option to continue calls with no application association is supported (see subclause 5.2.6) then the node shall invoke Gateway PINX functionality (see subclause 6.2.3.2.5). If this option is not supported, then the call shall be released and the management function shall be notified.

On reception of a PSS1_Error primitive containing an error notification indicating "reassembly error", the management function shall be notified.

On reception of a PSS1_Error indication primitive containing an error notification indicating "unrecognized information", then a call shall be allowed to proceed if possible, else the call shall be released.

6.2.6 Primitive Contents

Tables 6 to 7 contain the list of parameters in the primitives.

Table 8 shows the contents of the PSS1_Data primitive sent in conjunction with ISUP messages in a VPN call with support of PSS1 information flows continuity.

Mandatory/Optional (M/O) indications are provided as well as a reference for a detailed description of the parameters.

Table 6: Contents of the PSS1_Data Ind/Req primitive

Parameter	Mandatory/Optional
VPN feature transparency indication	O
Gateway PINX transformation capability	O
BGID	O
Gateway PINX request	O
ATII	M
SetupAcknowledgment	O
Calling party number	O
Called party number	O
Connected number	O
Facility (note)	O
Notification indicator (note)	O
Transit counter	O
NOTE: These parameters may be repeated.	

Table 7: Contents of the PSS1_Error/Ind primitive

Parameter	Mandatory/Optional
Error Notification	M

Table 8: Contents of the PSS1_Data Req./Ind primitives sent in conjunction with ISUP messages in a VPN call with support of PSS1 information flows continuity

ISUP message	PSS1_Data Req/ind primitive parameters (Mandatory/Optional)
IAM	• ATII (M) • Gateway PINX transformation capability (O) • BGID (O) • Calling party number (O) • Called party number (M) • Facility (O) (note) • Notification indicator (O) (note) • Transit counter (O)
ACM	• ATII (M) • VPN feature transparency indication (O) • Facility (O) (note) • Notification indicator (O) (note)
CPG	• ATII (M) • VPN feature transparency indication (O) • Facility (O) (note) • Notification indicator (O) (note)
ANM	• ATII (M) • VPN feature transparency indication (O) • Connected number (O) • Facility (O) (note) • Notification indicator (O) (note)
CON	• ATII (M) • VPN feature transparency indication (M in the PSS1_Data Request, O in the PSS1_Data Indication) • Connected number (O) • Facility (O) (note) • Notification indicator (O) (note)
PRI	• ATII (M) • VPN feature transparency indication (O) • Facility (O) (note) • Notification indicator (O) (note)
APM	• ATII (M) • VPN feature transparency indication (O) • Facility (if the Notification indicator parameter is not present M, else O) (note) • Notification indicator (if the Facility parameter is not present M, else O) (note)
NOTE: This parameter may be repeated.	

6.3 VPN Application Process functions - Connection without call (Bearer unrelated)

6.3.1 Introduction

The function of the public NNI support of VPN applications aspect of the application process is to co-ordinate between the VPN application process and the public application process functionality. When the private application requires the establishment of a signalling association without a bearer, the AP shall convert the private address information into the form that the public application process can use for routeing from the PIN to the appropriate node in the public network, PAN, which contains the adjacent PINX functionality. The PIN/PAN concept is described in EN 301 069-1 [9]. The specific private network use of the concept is described in subclause 5.1

. The conversion of private information to a form suitable for routeing through the public network is beyond the scope of the present document.

It is not the intention of the present document to re-define the PSS1 PINX functionality. The purpose of the present document is to describe how, through the use of TC and SCCP, the services expected by PSS1 at the GFT/PC interface (defined in ISO/IEC 11582 [3]) are fulfilled in a VPN, thus achieving PSS1 information flows continuity over the public NNI.

The PSS1 primitive interface between GFT and PC (see ISO model in ISO/IEC 11582 [3]) is not seen on any interface in the ALS. It is not the intention of the present document to model the AP; however to illustrate the relationship between the present document and the PINX functionality defined by ISO, figure 11 can be used.

Connectionless signalling is not supported by the present document.

6.3.2 Primitive Interface (AP - TC SACF)

The VPN application uses the services provided by the TC SACF primitive interface (interface (h) in figure 4) as listed in table 9.

Table 9: Primitives between AP and TC SACF

Primitive name	Types
PSS1_Setup	Indication/Request/Response/Confirmation
PSS1_Release	Indication/Request
PSS1_Reject	Indication/Request
PSS1_Facility	Indication/Request
PSS1_SetupAck	Indication/Request

6.3.3 Connection-oriented Signalling Procedures

The protocol control procedures that describe the mapping of the GFT primitives to transaction (TC) operations over the public NNI are described here with reference to ISO/IEC 11582 [3]. The procedural aspects of the PINX functionality are beyond the scope of the present document (see subclause 5.2.5 for the functionality provided by the VPN). In order to describe the relationship between the primitives on the GFT/PC interface to the operations used over TC, the present document defines the mapping between the primitives referred to in ISO/IEC 11582 [3] and the suitable AP/TC SACF interface primitives.

Primitives related to the private application functionality are beyond the scope of the present document (see ISO/IEC 11582 [3].

Table 10: Mapping between primitives used in ISO/IEC 11582 [3] and AP/TC SACF primitives

COLUMN A Primitives used at GFT/PC interfaced as defined in ISO/IEC 11582 [3]	COLUMN B Primitives used on AP/TC SACF interface
PC_SETUP request/indication	PSS1_SETUP request/indication
PC_SETUP response/confirmation	PSS1_SETUP response/confirmation
PC_RELEASE request/indication	PSS1_RELEASE request/indication
PC_REJECT request/indication	PSS1_REJECT request/indication
PC_DATA request/indication	PSS1_FACILITY request/indication
(not applicable)	PSS1_SetupAck request/indication

6.3.3.1 Business Group Identifier

The business group identifier shall either be supplied over the incoming UNI access, or it shall have an implicit value tied to the incoming access. The BGID is only required for call establishment (SETUP operation (TC)) and is mandatory over the international interface and has global significance. It is a network operator's option to employ an alternative mechanism for identifying a business group within its own domain. On receipt of a business group identifier that is not recognized by the PAN, the call shall be released with cause 63 (service or option not available - unspecified) and the management function notified.

6.3.3.2 Relay node

See subclause 6.2.3.4

6.3.4 Primitive contents

Tables 11 to 15 contain the list of parameters in the primitives.

The primitive PSS1_SetupAck is empty.

Mandatory/Optional (M/O) indications are provided as well as a reference for a detailed description of the parameters.

Table 11: Contents of the PSS1_SETUP Ind/Req

Parameter	Mandatory/Optional
Public Called Party Number	M
Called Party Number	M
Calling Party Number	O
Business Group Identifier	O
Facility (note)	O
Transit Counter	O
NOTE: This parameter may be repeated.	

Table 12: Contents of the PSS1_SETUP Res/Conf primitive

Parameter	Mandatory/Optional
Connected Number	O
Facility (note)	O
NOTE: This parameter may be repeated.	

Table 13: Contents of the PSS1_RELEASE Ind/Req primitive

Parameter	Mandatory/Optional
Cause	M
Facility (note)	O
NOTE: This parameter may be repeated.	

Table 14: Contents of the PSS1_REJECT Ind/Req primitive

Parameter	Mandatory/Optional
Cause	M
Facility (note)	O
NOTE: This parameter may be repeated.	

Table 15: Contents of the PSS1_FACILITY Ind/Req primitive

Parameter	Mandatory/Optional
Facility (note)	M
NOTE: This parameter may be repeated.	

7 Single Association Control Function (SACF) - ISUP SACF

7.1 Introduction

The main objective of ISUP SACF is to receive/deliver primitives from/to the appropriate entity and to perform a distribution function where appropriate for the ISUP AEI. The flow of information is from the AP (interface a) towards NI (interface f) or vice versa, therefore the SACF is also responsible for ensuring that, when multiple primitives are generated by the ASEs towards the AP, they are delivered across the interface together thus ensuring the correct associations are maintained. The SACF described here only defines the mapping and functions related to the NNI support of VPN applications aspect of the model. The SACF functionality related to the public APM functionality is beyond the scope of the present document. The mapping of primitives in tables 16 and 19 are in EN 301 069-1 [9] and are included here for informative purposes only.

The interfaces referenced herein are illustrated in subclause 5.2, figure 4. Examples of the "Dynamic primitive flows" can be found in the present document in subclause 5.2.3.

The primitives on the interface between SACF and the AP, (a) are defined in subclause 6.2.2

The parameters in these primitives are listed in tables 6 to 8.

The primitives on the interface between SACF and PSS1 ASE, (b) are defined in subclause 9.1.

The parameters in these primitives are listed in tables 24 to 25.

The primitives on the interface between SACF and UCEH ASE, interface (c) can be found in EN 301 069-1 [9] and are therefore beyond the scope of the present document.

The primitives on the interface between SACF and APM ASE, interface (d) can be found in EN 301 069-1 [9] and are therefore beyond the scope of the present document.

The primitives on the interface between SACF and ISUP ASE, interface (e) can be found in EN 301 069-1 [9] and are therefore beyond the scope of the present document.

The primitives on the interface between SACF and NI, interface (f) can be found in EN 301 069-1 [9] and are therefore beyond the scope of the present document.

7.2 Outgoing messages

On receipt of a primitive (request or response) from the AP (interface (a) in figure 4), the SACF issues appropriate primitive(s) to the ASEs, populating the parameters in the generated primitives from the appropriate subset of the parameters received from the AP. The SACF also performs distribution of the responding primitives received from the ASEs prior to sending the resulting primitive to NI (interface (f) in figure 4).

Table 16: Mapping between PSS1 ASE and APM ASE primitives

Interface (b), from PSS1 ASE	Interface (d), APM ASE
APM_U_Data	APM_Data

Table 17: Mapping between AP and PSS1 ASE primitives

Interface (a), from AP	Interface (b), PSS1 ASE
PSS1_Data	PSS1_Data

7.3 Incoming messages

These procedures are described in EN 301 069-1 [9] where the APM-user ASE corresponds with the PSS1 ASE.

Table 18: Mapping between PSS1 ASE and AP primitives

Interface (b), PSS1 ASE	Interface (a), from AP
PSS1_Data	PSS1_Data
PSS1_Error	PSS1_Error

Table 19: Mapping between APM ASE and PSS1 ASE primitives

Interface (d), from APM ASE	Interface (b), PSS1 ASE
APM_Data	APM_U_Data

Table 20: Mapping between UCEH ASE and PSS1 ASE primitives

Interface (c), from UCEH ASE	Interface (b), PSS1 ASE
APM_Error	APM_U_Error

8 Single Association Control Function (SACF) - TC SACF

8.1 Introduction

The main objective of TC SACF is to receive/deliver primitives from/to the appropriate entity for the TC AEI. The SACF described here only defines the mapping and functions related to the NNI support of VPN applications aspect of the model.

Four interfaces (shown in figure 4) are described by the present document.

- AP/SACF
- SCCP/SACF
- COPSS1/SACF
- TC ASE/SACF

The interfaces referenced herein are illustrated in subclause 5.2 figure 4. Subclause 5.2.3 also provides examples of the "Dynamic primitive flows".

The primitives received from the AP, on interface (h), are mapped as shown in subclauses 6.3.2 and 6.4.2. The parameters in these primitives are listed in subclause 6.3.5.

The primitives on the interface between SACF and COPSS1 ASE, (i) are listed in subclause 10.1.

The primitives on the interface between SACF and TCAP, (j) are listed in ETS 300 134 [13] (see clause 11).

The primitives on interface between SACF and SCCP, (k) are listed in ETS 300 009 [12] (see clause 12).

8.2 Outgoing operations

On receipt of a primitive (request or response) from the AP (interface (h) in figure 4), the SACF issues appropriate primitive(s) to the ASEs, populating the parameters in the generated primitives from the appropriate subset of the parameters received from the AP. The SACF also performs the distribution of the responding primitives received from the ASEs prior to sending the succeeding primitive. With regard to the interface between SACF and TCAP, all the TC primitives exchanged between the COPSS1 ASE and the TCAP pass through the SACF unchanged.

Table 21: Mapping between AP and COPSS1 ASE primitives

Interface (h), from AP	Interface (i), COPSS1 ASE
PSS1_Setup	PSS1_Setup
PSS1_SetupAck	PSS1_SetupAck
PSS1_Release	PSS1_Release
PSS1_Reject	PSS1_Reject
PSS1_Facility	PSS1_Facility

8.3 Incoming operations

On receipt of an N_DATA indication primitive from the SCCP, the SACF analyses the User Data field of this primitive according to the rules in ETS 300 009 [12]. It then proceeds to perform the function of distribution.

Table 22: Mapping between COPSS1 ASE and AP primitives

Interface (i), COPSS1 ASE	Interface (h), from AP
PSS1_Setup	PSS1_Setup
PSS1_SetupAck	PSS1_SetupAck
PSS1_Release	PSS1_Release
PSS1_Reject	PSS1_Reject
PSS1_Facility	PSS1_Facility

9 PSS1 ASE

The PSS1 ASE is responsible for the signalling aspects of the VPN application for the support of PSS1 information flows and for preparing the information in the appropriate form that can be passed to the APM for transportation.

9.1 Primitive interface

Table 23 lists the primitive interface between the PSS1 ASE and ISUP SACF (interface (b) in figure 4).

Table 23: Primitives between ISUP SACF and PSS1 ASE (APM)

Primitive name	Types
APM_U_Data	Indication/Request
APM_U_Error	Indication
PSS1_Error	Indication
PSS1_Data	Indication/Request

9.2 Signalling procedures

9.2.1 Public Initiating Node

9.2.1.1 Sending procedures

On reception of the PSS1_Data.request primitive, the PIN shall propose its contents in the appropriate format (see clause 13) and the context identifier value set to "PSS1 ASE (VPN)". The result shall be sent in the APM_U_Data.request primitive.

9.2.1.2 Receiving procedures

On reception of the APM_U_Data.indication primitive, its contents shall be checked for correct format and coding (see clause 13). If the check is passed, the received information shall be transferred and sent in the PSS1_Data.indication primitive. If the check is failed, then the PIN shall also send the PSS1_Error.indication primitive with the results and indicating "unrecognized information".

9.2.1.3 APM_U_Error primitive

On reception of the APM_U_Error.indication primitive, the contents should be passed unchanged in the PSS1_Error primitive.

9.2.2 Public Addressed Node

See subclause 9.2.1.

9.3 Primitive contents

Tables 24 and 25 list the mandatory and optional contents for the PSS1 ASE service primitives. These primitives are defined in EN 301 069-1 [9] and are included here for informative purposes only.

The contents of the PSS1_Error and PSS1_Data primitives are defined at the AP/SACF interface in subclause 6.2.6

Mandatory/Optional (M/O) indications are provided.

Table 24: Contents of the APM_U_Data Ind/Req primitive

Parameter	Mandatory/Optional
Application Context Identifier	M
Application Transport Instruction Indicators	M
Application Data	M

Table 25: Contents of the APM_U_Error/Ind primitive

Parameter	Mandatory/Optional
Notification	M

10 Connection-oriented PSS1 ASE (COPSS1 ASE)

This COPSS1 ASE is responsible for the signalling aspects of the VPN application for the support of PSS1 information flows, and for preparing the information in the appropriate form that can be passed to the TC for transportation.

10.1 TC-user sequence

In figure 12, a signalling flow is given for the setup and release of a dialogue to support bearer unrelated (connection-oriented) private network information transfer. The UNI information elements shall be transferred over the NNI using TC messages. The following operations are defined to allow the transfer of the relevant UNI information flows: ***setUp, connect, release, VPNTransport***. The setUp operation is of class 1 and the remaining operations are of class 4.

Two timers supervise the release of the TC dialogue. Timer T3 shall be started in the PIN on receipt of the setUp return result operation and timer T4 shall be started in the PAN on receipt of the setUp invoke operation. Both timers are restarted on sending or receiving an operation.

A class 3 operation called ***activityTest*** shall be sent to check whether the remote application is still alive. This operation shall be generated in the PIN on expiry of timer T3. Timer T2 shall supervise the receipt of the return result. On receipt of the activityTest operation the PAN shall restart timer T4 and on receipt of the return result the PIN shall stop timer T2 and start timer T3.

On expiry of timer T2 the PIN shall send a TC-END message and on expiry of timer T4 the PAN shall end the dialogue locally.

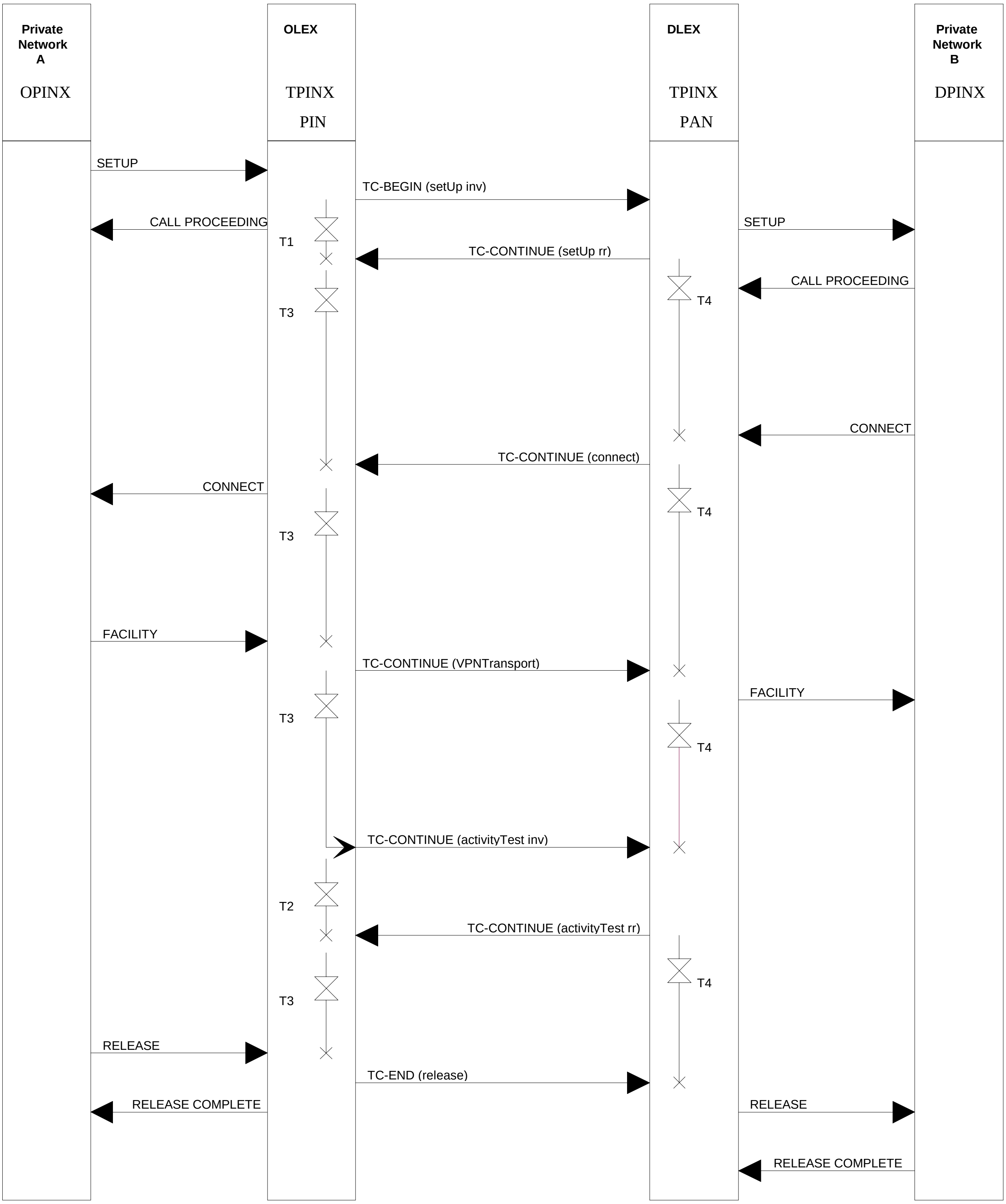


Figure 12: Example of a bearer unrelated signalling sequence

10.2 Interface COPSS1-ASE/SACF

Table 26 lists the primitive interface between the COPSS1-ASE and TC SACF (interface (i) in figure 4),

Other primitives on this interface correspond to the TC-user interface as defined in ETS 300 134 [13].

Table 26: Primitives between COPSS1-ASE and TC SACF (Protocol Control)

Primitive name	Types	Corresponding operation(s)
PSS1_SETUP	Indication/Request	SETUP.Invoke
PSS1_SETUP	Response/Confirmation	CONNECT.Invoke
PSS1_REJECT	Indication/Request	SETUP.ReturnResult
PSS1_SETUPACK	Indication/Request	SETUP.ReturnResult
PSS1_FACILITY	Indication/Request	VPNTRANSPORT.Invoke
PSS1_RELEASE	Indication/Request	RELEASE.Invoke

10.3 Supported Operations

The ASE supports the following Operations:

- SETUP	(Class 3)
- CONNECT	(Class 4)
- VPNTRANSPORT	(Class 4)
- RELEASE	(Class 4)
- ACTIVITYTEST	(Class 3)

Invocation of the above mentioned Operations can generate the following components:

- SETUP
  - SETUP. Invoke
  - SETUP.ReturnResult
- CONNECT
  - CONNECT.Invoke
- VPNTRANSPORT
  - VPNTRANSPORT.Invoke
- RELEASE
  - RELEASE.Invoke
- ACTIVITYTEST
  - ACTIVITYTEST.Invoke
  - ACTIVITYTEST.ReturnResult

10.4 ASE procedures

The COPSS1 ASE is responsible for co-ordinating the information received in primitives and preparing it according to the operation definition and TCAP primitive interface requirements.

10.4.1 Relationship between the COPSS1-ASE and TCAP

The dialogue defined for the PSS1 information flows support between the peer-to-peer entities (TC-Users) is a structured dialogue. The dialogue ID parameter is used in both operation handling and transmission (dialogue) handling primitives to determine which component(s) pertain(s) to which dialogue.

Each TC-User has its own reference for a given dialogue. These references are local references and mapping of these local references into protocol references transaction ID, included in the messages, shall be done by TC.

All the operations below relate to the same dialogue.

Class 3 and 4 operations are used.

Each TC message conveys only a single operation.

10.4.1.1 Dialogue beginning

The PIN establishes the dialogue by using a TC-BEGIN.request primitive with TC-INVOKE.request primitive to transmit a SETUP (class 3) operation invoke component to the PAN. The PAN responds by:

- Using the TC-CONTINUE.request primitive with TC-RESULT-L.request primitive to transmit a SETUP.ReturnResult component, confirm the dialogue, and indicate that the SETUP.request operation was successful. No parameter is included in this case in the SETUP.ReturnResult.
- Using the TC-END.request primitive with TC-RESULT-L.request primitive to transmit a SETUP.ReturnResult component, end the dialogue, and indicate that the SETUP.request operation failed. The cause parameter is included in this case. In addition, one or more Facility "Networking extensions" information elements may be included in the vpnTransport parameter.

10.4.1.2 Dialogue continuing

The continuation of the dialogue is assumed by the CONNECT (Class 4), VPNTRANSPORT (Class 4) and ACTIVITYTEST (Class 3) operations using TC-CONTINUE primitives.

10.4.1.3 Dialogue end

10.4.1.3.1 Basic End

A dialogue end is requested by either the PIN or PAN using TC_END.request primitive with TC-INVOKE.request primitive to transmit a RELEASE operation invoke component.

10.4.1.3.2 Abnormal End

When the TC-user determines that it will abort the dialogue, it does so with the TC-U-ABORT primitive. On receipt of a TC-NOTICE or a TC-P-ABORT indication primitive, the TC dialogue shall be terminated.

10.4.2 Operations

10.4.2.1 Setup operation

On reception of the PSS1_SETUP.request primitive, its contents are loaded into and sent from the PIN with the SETUP.invoke operation. Timer T1 is started. On reception of the operation at the PAN, its contents are sent in a PSS1_SETUP.indication primitive. In case the signalling connection request can be accepted by the AP at the PAN (the COPSS1 ASE receives a PSS1_SETUPACK request), it responds towards the PIN with the SETUP.ReturnResult operation and starts timer T4. On reception of the return result operation at the PIN, its contents are sent in a PSS1_SETUPACK.indication, timer T1 is stopped, and timer T3 is started. In case the signalling connection request cannot be accepted by the AP at the PAN (the COPSS1 ASE receives a PSS1_REJECT request), it responds towards the PIN with the SETUP.ReturnResult operation. On reception of the return result operation at the PIN, its contents are sent in a PSS1_REJECT indication and timer T1 is stopped.

10.4.2.2 Connect operation

On reception of the first PSS1_SETUP.response primitive, its contents are loaded into and sent from the PAN with the CONNECT.invoke. Timer T4 is restarted. On reception of the operation at the PIN, the contents are passed in the PSS1_SETUP.confirmation primitive, timer T3 is restarted.

10.4.2.3 VPNTransport operation

The VPNTransport operation may be sent from either PIN to PAN or vice versa after sending/receipt of the CONNECT invoke operation.

PIN to PAN: On reception of the PSS1_FACILITY.request primitive, its contents are loaded into and sent from the PIN with the VPNTRANSPORT.invoke operation. Timer T3 is restarted. On reception of the operation at the PAN, the contents are passed in the PSS1_FACILITY.indication primitive, and timer T4 is restarted.

PAN to PIN: On reception of the PSS1_FACILITY.request primitive, its contents are loaded into and sent from the PAN with the VPNTRANSPORT.invoke. Timer T4 is restarted. On reception of the operation at the PIN, the contents are passed in the PSS1_FACILITY.indication primitive, and timer T3 is restarted.

10.4.2.4 ActivityTest operation

On expiry of timer T3, the PIN sends an ACTIVITYTEST.invoke operation and starts timer T2. On reception of the operation, the PAN sends the ACTIVITYTEST.returnresult operation in response and restarts timer T4. On reception of the response at the PIN, timer T2 is stopped and timer T3 started.

10.4.2.5 Release operation

The RELEASE operation may be sent from either PIN to PAN or vice versa.

PIN to PAN: On reception of the PSS1_RELEASE.request primitive, its contents are loaded into and sent from the PIN with the RELEASE.invoke operation. Timer T3 is stopped. On reception of the operation at the PAN, the contents are passed in the PSS1_RELEASE.indication primitive, and timer T4 is stopped.

PAN to PIN: On reception of the PSS1_RELEASE.request primitive, its contents are loaded into and sent from the PAN with the RELEASE.invoke operation. Timer T4 is stopped. On reception of the operation at the PIN, the contents are passed in the PSS1_RELEASE.indication primitive, and timer T3 is stopped.

10.4.2.6 Exceptional procedures

On receipt of either a TC-P-ABORT, a TC-U-ABORT, a TC-U-REJECT, a TC-L-CANCEL or a TC-NOTICE primitive the dialogue is released with cause "normal unspecified".

10.4.3 Expiry of timers

10.4.3.1 T1

On expiry of timer T1, the dialogue shall be aborted locally using the TC-U-ABORT primitive and the PSS1_REJECT indication primitive shall be sent to the Application Process with cause "normal unspecified".

10.4.3.2 T2

On expiry of timer T2, the dialogue shall be aborted locally using the TC-U-ABORT primitive and the PSS1_RELEASE indication primitive shall be sent to the Application Process with cause "normal unspecified".

10.4.3.3 T3

On expiry of timer T3, the activity test procedures shall be initiated (see subclause 10.4.2.4).

10.4.3.4 T4

On expiry of timer T4, the dialogue shall be aborted locally using the TC-U-ABORT primitive and the PSS1_RELEASE indication primitive shall be sent to the Application Process with cause "normal unspecified".

10.4.4 Signalling congestion

In order to avoid signalling link congestion in the No.7 network, it is necessary that applications that contribute signalling load towards a congested link limit such signalling in a controlled manner. On receipt of a congestion indication (TC-NOTICE primitive indicating signalling congestion) the application shall reduce signalling traffic load in several steps.

When the first congestion indication is received by the application, the signalling traffic load shall be reduced by one step. At the same time two timers T-C1 and T-C2 shall be started. During T-C1 all received congestion indications shall be ignored in order not to reduce traffic too rapidly. Reception of a congestion indication after the expiry of T-C1, but still during T-C2, shall decrease the signalling load by one more step and restart T-C1 and T-C2. This step wise reduction of the application signalling load shall be continued until maximum reduction is obtained by arriving at the last step. If T-C2 expires (i.e. no congestion indications having been received during the T-C2 period) signalling load shall be increased by one step and T-C2 shall be restarted unless full signalling load has been resumed.

Timers T-C1 and T-C2 have the following recommended range:

T-C3 = 300-600 ms;

T-C4 = 5-10 s.

The number of steps of traffic reduction and the type and/or amount of increase/decrease of traffic load at the various steps are considered to be implementation matters. The steps change with respect to the timers and the reception of the TC-NOTICE primitive indicating "signalling congestion".

The two timer method, as described above would allow for a smooth reduction and resumption of signalling towards the MTP in the case of congestion.

The use of different timer values for different applications would allow for a mechanism of prioritization of the applications. These timer values should be definable by the operator.

10.5 Primitive contents

The contents of the primitives are described in subclause 6.3.4.

10.6 Abstract syntax, general

Subclause 10.8 specifies the abstract syntax for the COPSS1 ASE protocol using the Abstract Syntax Notation One (ASN.1), see CCITT Recommendation X.208 [15].

The set of values each of which is a value of the ASN.1 type TCAPMessages, MessageType as defined in ETS 300 134 [13]with the ANY DEFINED BY definitions resolved by the operations and errors definitions included in subclause 10.8 form the abstract syntax for the COPSS1 ASE protocol.

The set of encoding rules which are applicable to this abstract syntax are defined by ETS 300 134 [13]. The mapping of the OPERATION and ERROR MACROs to TC components is also described in ETS 300 134 [13].

The ASN.1 data type which follows the keywords "PARAMETER" or "RESULT" (for OPERATION and ERROR) is always optional from a syntactic point of view. However, except for specific mention, it has to be considered as mandatory from a semantic point of view.

When a mandatory element is missing in any component or inner data structure, a reject component is returned (if the dialogue still exists). The problem cause to be used is "Mistyped parameter".

10.7 Subsystem number

The SSN value of 0000 1011 "ISDN supplementary services" is to be used

10.8 ASN.1 module

The following ASN.1 module specifies the protocol elements defined for the COPSS1 ASE. It shows the definition of the operations, errors and types required for the connection-oriented, bearer unrelated signalling for the support of PSS1 information flows using ASN.1 as defined by CCITT Recommendation X.208 [15] and using the OPERATION and ERROR macros as defined by ETS 300 134 [13].

The formal definition of the component types to encode these operations, errors and types is provided in ETS 300 134 [13].

```
COPSS1-Protocol {itu-t recommendation q vpn modules(2) operations-and-errors(1) version1(1)}
DEFINITIONS IMPLICIT TAGS   ::=
BEGIN
IMPORTS OPERATION, ERROR
            FROM TCAP Messages {ccitt recommendation q 773 modules(2) messages(1) version2(2)};
====================================================================================
-- TYPE DEFINITIONS FOR OPERATIONS
====================================================================================
-- Specification of SetUp
-- =================
-- Direction:   OLEX -> DLEX
-- Class:   1
-- Timer:   T1
-- Purpose: To be provided.
SetUp           ::= OPERATION
    ARGUMENT
        SetUpArg
    RESULT
        SetUpResultArg
-- Specification of Connect
-- ==================
-- Direction:   DLEX -> OLEX
-- Class:   4
-- Purpose: To be provided.
Connect    ::= OPERATION
    ARGUMENT
        ConnectArg
-- Specification of Release
-- ==================
-- Direction:   OLEX -> DLEX and DLEX -> OLEX
-- Class:   4
-- Purpose: To be provided.
Release         ::= OPERATION
    ARGUMENT
        ReleaseArg
-- Specification of VpnTransport
-- ====================
-- Direction:   OLEX -> DLEX and DLEX -> OLEX
-- Class:   4
-- Purpose: To be provided.
VpnTransport        ::= OPERATION
    ARGUMENT
        VpnFacilityArg
-- Specification of ActivityTest
-- =====================
-- Direction:   OLEX -> DLEX
-- Class:   3
-- Timer:   T2
-- Purpose: To be provided.
ActivityTest        ::= OPERATION
    RESULT
====================================================================================
-- TYPE DEFINITIONS FOR ERRORS
====================================================================================
-
====================================================================================
-- TYPE DEFINITIONS FOR ARGUMENT DATA
====================================================================================
SetUpArg            ::= SEQUENCE {
    calledPartyNumber       [0] CalledPartyNumber,
    VPNTransport        [1] VPNTransport,
    ...
    }
```

```
SetUpResultArg      ::= SEQUENCE {
    cause           [0] Cause OPTIONAL,
    vpntransport        [1] VPNTransport OPTIONAL,
    ...
    }
ConnectArg          ::= VPNTransport
ReleaseArg          ::= SEQUENCE {
    cause               [0] Cause,
    vpntransport            [1] VPNTransport OPTIONAL,
    ... }
VpnFacilityArg      ::= VPNTransport
====================================================================================
-- TYPE DEFINITIONS FOR DATA
====================================================================================
CalledPartyNumber   ::= OCTET STRING (SIZE (1..maxcdPlength))
    -- The CalledPartyNumber is coded as described in Q.763 [4].
VPNTransport    ::= OCTET STRING (SIZE (0..maxlength))
    -- The VPNTransport is coded as described in section 13/Q.vpn.
Cause           ::= OCTET STRING (SIZE (1..maxCauseLength)) -- The Cause is coded as described in
ISO/IEC 11572 [2]/ Q.931 Annex Q [28]
====================================================================================
-- DEFINITION OF RANGE CONSTANTS
====================================================================================
maxCauseLength          INTEGER ::= 32
maxLength               INTEGER ::= 2048
maxcdPlength            INTEGER::= Network specific
====================================================================================
-- DEFINITION OF OBJECT IDENTIFIER PATH
====================================================================================
COPSS1OID       OBJECT IDENTIFIER   ::= {itu-t recommendation q vpn operations-and-errors(1)}
====================================================================================
-- ASSIGNMENTS FOR OPERATION VALUES
====================================================================================
setUp           SetUp           ::= globalValue {COPSS1OID setUp(1)}
connect     Connect     ::= globalValue { COPSS1OID connect(2)}
release     Release     ::= globalValue { COPSS1OID release(3)}
vpnFacility     VpnFacility     ::= globalValue { COPSS1OID vpnFacility(4)}
activityTest        ActivityTest        ::= globalValue { COPSS1OID activityTest(5)}
====================================================================================
-- ASSIGNMENTS FOR ERROR VALUES
====================================================================================
-
END -- of COPSS1-Protocol
```

11 TCAP (TC ASE)

The SACF uses the services provided by the TCAP primitive interface. The definition of TCAP is beyond the scope of the present document. For details refer to ETS 300 134 [13].

11.1 Interface TCAP/SACF

11.1.1 Primitives

The primitives at this interface that support the services offered by TCAP are defined in ETS 300 134 [13].

11.1.2 Use of TCAP

This application uses TCAP for structured dialogues.

The peer-to-peer dialogue established by the COPSS1 ASE, as a TC-user, is a structured dialogue. The dialogue ID parameter is used in both operation handling and transmission (dialogue) handling primitives to determine which component(s) pertain(s) to which dialogue. Each TC-user has its own reference for a given dialogue. These references are local references and mapping of these local references into protocol references transaction ID, included in the messages, is done by TCAP. The class used by each operation is defined in the ASN.1 definition.

12 SCCP

12.1 Interface SCCP/SACF

The TC-SACF uses the services provided by the SCCP primitive interface. The definition of SCCP is beyond the scope of the present document. For details refer to the SCCP ETS 300 009 [12].

12.2 Use of SCCP

- SCCP Class 1 service (Sequenced Connectionless Service) is used by this application.
- The SCCP message return option will always be used.
- A minimum of the 1992 version of SCCP to be used, but preferably 1996/7 version of SCCP (ETS 300 009 [12]) to be used.

12.3 Routeing in the SCCP network

For routeing on the international interface and for routeing based on the GT translation mechanism within national networks, the coding of the called party address and the calling party address in SCCP shall comply with the following restrictions:

SSN indicator	1	(SSN for ISDN supplementary services is always included)
GT indicator	0100	(includes translation type numbering plan encoding scheme and nature of address)
Translation Type	0001 0001	(translation table)
Numbering plan	0001	(ISDN/Telephony Numbering Plan E.164)
Routeing indicator	0	(Routeing on global title)

Alternatively, for routeing within a national network, the SCCP addressing method based on SPCs may apply. However, within large national networks, it would be advisable to use a hybrid addressing method based on SPCs for regional traffic and GT translation mechanism for long distance traffic, to keep the SS7 routeing data manageable.

12.4 Number Information used for routeing

The exchange which initiates a dialogue using the GT translation mechanism, shall give an E.164 address as GT in the SCCP calling address field which will uniquely identify it. For routeing on the international interface, the number information used for GT translation shall comply to the E.164 numbering schemes for Country code and National destination code.

13 VPNTransport - formats and codes of application data

The following defines the formats and codes for the support of the VPN application for the support of PSS1 information flows as an APM-user. The information structure defined here is passed as Application Data to the underlying transport mechanism (APM) in the APM_U_Data primitive. The Application Context Identifier field of the Application Transport parameter (APP) shall be coded "PSS1 ASE (VPN)".

The Encapsulated Application Information field within the APP and the VPNTransport are coded identically. The format is such that it can provide a service of transparent transport of information (i.e. PSS1 information elements) as well as having the ability of passing additional network related information within the public network. The Application information is structured such that the first octet is a pointer to the PSS1 information to be transported transparently (see subclause 13.1). The pointer value (in binary) gives the number of octets between the pointer octet itself (included) and the first octet (not included) of transparent PSS1 data. The pointer value of zero is used to indicate that, no transparent PSS1 data is present. The range of octets between the pointer octet and the first octet of transparent PSS1 data (to which the pointer octet points) contains the network related information (see subclause 13.2) to be passed between VPN applications residing within the public network.

13.1 Private network specific information elements to be transported within the Application Transport Parameter

The transparent transport of PSS1 information flows within the APP is achieved by transporting the information elements in table 27.

Table 27: PSS1 information elements transported within the APP

Information Element	Ref.	Type	Length
Calling party number	[2]/[6] (i)	O	4-*
Called party number	[2]/[6](i)	O	4-*
Connected number	[2]/[6](i)	O	4-*
Facility with protocol profile value set to "Networking extensions" (ii)	[3]/[6](i)	O	3-*
Notification indicator (ii)	[3]/[6](i)	O	3-*
Non-locking Shift	[3]/[6](i)	O	1
Transit counter	[26]/[6](i)	O	3-*
NOTE 1: (i) The definition of these information elements by ISO/IEC 11572 [2], 11582 [3], 15055 [5] and by ETS 300 403-1 [6], ETS 300 196 [7] are identical and therefore equally applicable. NOTE 2: (ii) These information elements may be repeated.			

13.2 NNI specific Information to be transported in the Application Transport Parameter

The NNI specific information for the VPN application is carried within the APP in the following manner.

	8	7	6	5	4	3	2	1
1	Ext	spare			SAI	GR	GT	VTI
2	BGID length							
3 : 14	BGID							

a) VPN feature transparency indication (VTI)

0 no indication

1 call with VPN feature transparency capability;

b) Gateway PINX Transformation capability (GT)

0 no indication

1 PINX with Gateway transformation capability

c) Gateway PINX request indication (GR)

0 no indication

1 Gateway PINX transformation request

d) Setup Acknowledgement Indicator

0 no indication

1 Setup acknowledgement

e) Extension indicator (Ext)

0 information continues through the next octet

1 last octet

f) BGID length

number of octets containing BGID

g) BGID

Binary value

NOTE: The BGID begins with the binary coded decimal (BCD) representation of the E.164 country code digits of the country where the business group was initially assigned.

14 Timers

This clause specifies all the Application Process and Protocol timers relevant for VPN applications. For each timer the timeout value, cause or initiation of that timer, normal termination event(s) for the timer, and actions to be performed on expiry of the timer, are given. Furthermore, in the last column reference to the relevant Application Process description, or ASE description is given, where a full description of the procedure is to be found.

14.1 Timers in ISUP

Table 28: Timers in ISUP

Symbol	Time-out value	Cause for initiation	Normal termination	At expiry	Subclause
T-C1	300 - 600 ms	Reception of "signalling congestion" indication	Expiry of T-C1	Act upon subsequent "signalling congestion" indications whilst T-C2 is still running	6.2.4.1
T-C2	5 - 10 s	Reception of "signalling congestion" indication and on expiry of T-C2 unless full signalling load has been reached	Expiry of T-C2 (when full signalling load has been reached)	Increase signalling load by one step. Restart T-C2 if not carrying full signalling load	6.2.4.1

14.2 Timers in TC-USER

Table 29: Timers in TC-user

Symbol	Time-out value	Cause for initiation	Normal termination	At expiry	Subclause
T1	1 - 5 s	Sending of SETUP.Invoke	Reception of SETUP.ReturnResult	Abort dialogue locally Inform management function	10.4.3.1
T2	1 - 5 s	Sending of ActivityTest.invoke	Reception of ActivityTest.ReturnResult	Send TC-END Inform management function1	10.4.3.2
T3	10 - 60 min	Reception of Setup.ReturnResult Connect.Invoke VPNtransport.Invoke ActivityTest.ReturnResult Sending of VPNtransport.Invoke	Reception of Connect.Invoke VPNtransport.Invoke Release.Invoke Sending of ActivityTest.Invoke	Send ActivityTest.Invoke	10.4.3.3
T4	10 - 60 min (Note T4 must be greater than T3)	Reception of VPNtransport.Invoke Sending of Setup.ReturnResult Connect.Invoke VPNtransport.Invoke ActivityTest.ReturnResult	Reception of ActivityTest.Invoke Sending of Connect.Invoke VPNtransport.Invoke Release.Invoke	Abort dialogue locally Inform management function	10.4.3.4
T-C3	300 - 600 ms	Reception of "signalling congestion" indication	Expiry of T-C3	Act upon subsequent "signalling congestion" indications whilst T-C4 is still running	10.4.4
T-C4	5 - 10 s	Reception of "signalling congestion" indication and on expiry of T-C4 unless full signalling load has been reached	Expiry of T-C4 (when full signalling load has been reached)	Increase signalling load by one step. Restart T-C4 if not carrying full signalling load	10.4.4

Annex A (informative): Signalling interworking specification for ISUP

A.1 Introduction

The following subclauses specify the interworking between Signalling System No. 7 ISDN User Part (ISUP) version 3 and extended Digital Subscriber Signalling System No. one (DSS1) defined in EN 300 356-1 [8] and ETS 300 403-1 [6] for the support of private network interconnection in VPN applications.

These interworking procedures are defined as delta procedures to ETS 300 899 [11].

The ISUP - DSS1 interworking procedures specified in ETS 300 899 [11] shall apply to the interworking between ISUP and extended DSS1 defined in EN 300 356-1 [8] and ETS 300 403-1 [6] with the following modifications.

NOTE: The description of the ISUP - extended DSS1 interworking with reference to ISUP V2 interworking document (ETS 300 899 [11]) may not fully cover all interworking aspects since the ISUP V3 specific basic call and supplementary services interworking aspects are not documented in this ETS.

A.2 Methodology

APM-user information segmentation:

The actions described in the following subclauses on receipt of Application Transport parameters (APP) take place only after the completion of the segmentation and reassembly procedure specified in clause 9.

When it is said in the text that an APP parameter is received in an ISUP message, in case of segmentation it could be received as well in an APM containing segmented information linked to that message.

A.3 Outgoing Call

A.3.1 Sending of the Initial Address Message (IAM)

If the access has extended DSS1 capability and if the exchange has determined that it is a VPN call requesting support of PSS1 information flows, the IAM sent is coded as described in subclause 2.1.1.1/ETS 300 899 [11] with the following modifications.

Called party number

Add the following sentence:

The called party number parameter is generated by the VPN Application Process.

Application Transport

Table A.1: Contents of the Application Transport parameter

SETUP→	**IAM→**
Content	Application Transport parameter
	Application Context Identifier "PSS1 ASE (VPN)"
	Gateway PINX Transformation capability (note 1)
	Business Group Identifier (note 2)
Non-locking shift	Non-locking shift
Transit counter	Transit counter
Calling party number	Calling party number
Called party number	Called party number
Facility with Protocol profile value set to "Networking Extensions"	Facility with Protocol profile value set to "Networking Extensions"
Notification indicator	Notification indicator

NOTE 1: The "Gateway PINX Transformation capability" indication is optional and is coded as described in clause 13.

NOTE 2: The Business Group Identifier is optional. When present, it consists of two fields (BGID length and BGID, as described in clause 13) and its value is either derived from information received from the calling user in the VPN indicator information element in the SETUP message or is an implicit value tied to the incoming access.

Generic number

Replace item about Generic number in subclause 2.1.1.1/ETS 300 899 [11] by:

> The calling party number received in the calling party number information element of the SETUP message is transferred in the generic number parameter with the number qualifier indicator coded "additional calling party number" without taking into account the public CLIR and the CLIP supplementary services.
>
> The called party number received in the called party number information element of the SETUP message is transferred in the generic number parameter with the number qualifier indicator coded "additional called party number".

NOTE: The coding "Private numbering plan" may be used in the numbering plan indicator of the generic number parameter.

A.3.2 VPN call with VPN feature transparency

The originating exchange knows that the VPN call does support PSS1 information flows continuity when the VPN feature transparency indication is received coded "Call with VPN feature transparency capability" in a application transport parameter with the Application Context Identifier coded "PSS1 ASE (VPN)" in the address complete message (ACM) or in a call progress message (CPG) or in the connect message (CON) or in the answer message (ANM) or in the pre-release information message (PRI) or in a Application Transport message (APM).

From the receipt of this explicit information, the originating exchange shall apply the provisions of the following subclauses.

A.3.2.1 Receipt of the Address complete message (ACM)

Upon receipt of an address complete message (ACM), the exchange shall apply the actions described in *subclause* 2.1.1.3/*ETS 300 899 [11]* with the following modifications.

Facility/Notification indicator

Add the following table:

Table A.2: Transfer of the Facility/Notification indicator information element

←Appropriate DSS1 message	←ACM
Content	Application Transport parameter
	Application Context Identifier "PSS1 ASE (VPN)"
Facility	Facility
Notification indicator	Notification indicator

A.3.2.2 Receipt of the Call progress message (CPG)

Upon receipt of a call progress message (CPG), the exchange shall apply the actions described in *subclause* 2.1.1.4/*ETS 300 899 [11]* with the following modifications.

Facility/Notification indicator

Add the following table:

Table A.3: Transfer of the Facility/Notification indicator information element

←Appropriate DSS1 message	←CPG
Content	Application Transport parameter
	Application Context Identifier "PSS1 ASE (VPN)"
Facility	Facility
Notification indicator	Notification indicator

A.3.2.3 Receipt of the Answer message (ANM)

Upon receipt of an answer message (ANM), the exchange shall apply the actions described in *subclause* 2.1.1.5/*ETS 300 899 [11]* with the following modifications.

Connected number

Replace item about Connected number in subclause 2.1.1.5/ETS 300 899 [11] by:

> The connected number information element received in the application transport parameter is transferred in the CONNECT message without taking into account any possible public COLP supplementary service provision or restriction (COLR).

Table A.4: Transfer of the Connected number information element

←CONNECT	←ANM
Content	Application Transport parameter
	Application Context Identifier "PSS1 ASE (VPN)"
Connected number	Connected number

Connected sub-address

Replace item about Connected sub-address in subclause 2.1.1.5/ETS 300 899 [11] by:

> The connected subaddress information element received in the access transport parameter is passed on in the CONNECT message without taking into account any possible public COLP supplementary service provision or restriction (COLR).

Facility/Notification indicator

Add the following table:

Table A.5: Transfer of the Facility/Notification indicator information element

←CONNECT	←ANM
Content	Application Transport parameter
	Application Context Identifier "PSS1 ASE (VPN)"
Facility	Facility
Notification indicator	Notification indicator

A.3.2.4 Receipt of the Connect message (CON)

Upon receipt of a connect message (CON), the exchange applies the actions described in *subclause* 2.1.1.6/ETS 300 899 [11] with the following modifications.

Connected number

Replace item about Connected number in subclause 2.1.1.6/ETS 300 899 [11] by:

> The connected number information element received in the application transport parameter is transferred in the CONNECT message without taking into account any possible public COLP supplementary service provision or restriction (COLR).

Table A.6: Transfer of the Connected number information element

←CONNECT	←CON
Content	Application Transport parameter
	Application Context Identifier "PSS1 ASE (VPN)"
Connected number	Connected number

Connected sub-address

Replace item about Connected sub-address in subclause 2.1.1.6/ETS 300 899 [11] by:

> The connected subaddress information element received in the access transport parameter is passed on in the CONNECT message without taking into account any possible public COLP supplementary service provision or restriction (COLR).

Facility/Notification indicator

Add the following table:

Table A.7: Transfer of the Facility/Notification indicator information element

←CONNECT	←CON
Content	Application Transport parameter
	Application Context Identifier "PSS1 ASE (VPN)"
Facility	Facility
Notification indicator	Notification indicator

A.3.2.5 Receipt of the Application Transport message

Upon receipt of a Application Transport message with the Application Context Identifier coded "PSS1 ASE (VPN)", the exchange transfers the following information in a FACILITY message or in a NOTIFY message.

Table A.8: Receipt of the Application Transport message

←FACILITY/NOTIFY	←Application Transport
Content	Application Transport parameter
	Application Context Identifier "PSS1 ASE (VPN)"
Facility	Facility
Notification indicator	Notification indicator
NOTE: The Application Transport message may be received in any state of the call.	

A.3.2.6 Sending of the Application Transport message

Upon receipt of a FACILITY message or a NOTIFY message, the exchange transfers the following information in a Application Transport message.

Table A.9: Sending of the Application Transport message

FACILITY/NOTIFY→	Application Transport→
Content	Application Transport parameter
	Application Context Identifier "PSS1 ASE (VPN)"
Facility with Protocol profile value set to "Networking Extensions"	Facility with Protocol profile value set to "Networking Extensions"
Notification indicator	Notification indicator

A.3.2.7 Receipt of the Release message (REL)

The actions described in subclause 2.1.1.7/ETS 300 899 [11] applies with the following additions:

Upon receipt of a release message (REL) subsequent to a pre-release information message (PRI), the exchange shall transfer the following information in a DISCONNECT message.

Facility/Notification indicator

Table A.10: Sending of the DISCONNECT message

←DISCONNECT	←REL subsequent to a PRI message
Content	Application Transport parameter received in the PRI message
	Application Context Identifier "PSS1 ASE (VPN)"
Facility	Facility
Notification indicator	Notification indicator

A.3.2.8 Sending of the Pre-release information message (PRI)

Upon receipt of a DISCONNECT, RELEASE or RELEASE COMPLETE message, the exchange shall transfer the following information in a pre-release information message (PRI) before sending the release message.

Application Transport

Table A.11: Sending of the Pre-release information message

DISCONNECT, RELEASE, RELEASE COMPLETE→	PRI→
Content	Application Transport parameter
	Application Context Identifier "PSS1 ASE (VPN)"
Facility with Protocol profile value set to "Networking Extensions"	Facility with Protocol profile value set to "Networking Extensions"
Notification indicator	Notification indicator

A.4 Incoming Call

A.4.1 VPN call with VPN feature transparency

If the initial address message (IAM) received contains the Application Transport parameter with the Application Context Identifier coded "PSS1 ASE (VPN)" and if the called access has the extended DSS1 capability, the exchange shall apply the following subclauses.

A.4.1.1 Sending of the SETUP message

The actions described in subclause 3.1.1.1/ETS 300 899 [11] shall apply with the following modifications:

Calling party number

Replace item about Calling party number in subclause 3.1.1.1/ETS 300 899 [11] by:

The calling party number information element received in the application transport parameter is transferred in the SETUP message without taking into account any possible public CLIP supplementary service provision or restriction (CLIR).

If the two calling party number delivery option defined in the public CLIP supplementary service applies, two Calling party number information elements are sent on DSS1 side:

- the first one coded as received in the application transport parameter;
- the second one coded according to the calling party number parameter as defined in subclause 3.1.2.3/ETS 300 899 [11] when the generic number parameter with number qualifier set to "additional calling party number" is absent.

Calling party subaddress

Replace item about Calling party subaddress in subclause 3.1.1.1/ETS 300 899 [11] by:

> The calling party subaddress information element received in the access transport parameter is passed on in the SETUP message without taking into account any possible public CLIP supplementary service provision or restriction (CLIR).

Called party number

Replace item about Called party number in subclause 3.1.1.1/ETS 300 899 [11] by:

Table A.12: Transfer of the Called party number information element

IAM→	SETUP→
Application Transport parameter	Content
Application Context Identifier "PSS1 ASE (VPN)"	
Called party number	Called party number

Transit counter

> The non-locking shift information element followed by the transit counter information element received in the Application Transport parameter are passed on unchanged in the SETUP message.

Facility/Notification indicator

Add the following table:

Table A13: Transfer of the Facility/Notification indicator information element

IAM→	SETUP→
Application Transport parameter	Content
Application Context Identifier "PSS1 ASE (VPN)"	
Facility	Facility
Notification indicator	Notification indicator

A.4.1.2 Sending of the Address complete message (ACM)

The actions described in subclause 3.1.1.3/ETS 300 899 [11] applies with the following modifications:

Replace the first paragraph in subclause 3.1.1.3/ETS 300 899 [11] by:

The following cases are possible trigger conditions of sending the address complete message (ACM):

a) the destination exchange has determined independently of access indications that the complete called party number has been received;

b) overlap receiving is used on the DSS1 side and a CALL PROCEEDING is received;

c) en-bloc receiving is used on the DSS1 side and a Progress indicator information element is received in a CALL PROCEEDING message (except with value No. 8 *In-band information or an appropriate pattern is now available*, No. 3 *originating address is non-ISDN*, or No. 4 *call has returned to the ISDN*) or in a PROGRESS message (except with value No. 3 *originating address is non-ISDN*, or No. 4 *call has returned to the ISDN*);

d) the first ALERTING message is received;

e) it has been determined, in case of call failure, that a special in-band tone or announcement has to be returned to the calling party from the destination exchange.

Access transport

Replace the first sentence of item about Access transport in subclause 3.1.1.3/ETS 300 899 [11] by:

This parameter carries the Progress indicator information element possibly received from the called user.

Application Transport

Table A.14: Contents of the Application Transport parameter

←ACM	←Message received from the access
Application Transport	Content
Application Context Identifier "PSS1 ASE (VPN)"	
VPN feature transparency indication "Call with VPN feature transparency capability" (note)	
Facility with Protocol profile value set to "Networking Extensions"	Facility with Protocol profile value set to "Networking Extensions"
Notification indicator	Notification indicator
NOTE: Only included if the address complete message (ACM) is the first backwards message sent by the destination exchange.	

A.4.1.3 Sending of the Call progress message (CPG)

The actions described in subclause 3.1.1.4/ETS 300 899 [11] applies with the following modifications:

Replace the first paragraph in subclause 3.1.1.4/ETS 300 899 [11] by:

If the address complete message (ACM) has already been sent, the following cases are possible trigger conditions of sending the CPG:

a) it has been determined that an in-band tone or announcement has to be returned to the calling party from the destination exchange;

b) receipt of a Progress indicator information element in a CALL PROCEEDING message (except with value No. 8 *In-band information or an appropriate pattern is now available*, No. 3 *originating address is non-ISDN*, or No. 4 *call has returned to the ISDN*) or in a PROGRESS message (except with value No. 3 *originating address is non-ISDN*);

c) receipt of the first ALERTING message.

Application Transport

Table A.15: Contents of the Application Transport parameter

←CPG	**←Message received from the access**
Application Transport	Content
Application Context Identifier "PSS1 ASE (VPN)"	
Facility with Protocol profile value set to "Networking Extensions"	Facility with Protocol profile value set to "Networking Extensions"
Notification indicator	Notification indicator

A.4.1.4 Sending of the Answer message (ANM)

The answer message (ANM) is coded as described in subclause 3.1.1.5/ETS 300 899 [11] with the following modifications.

Generic number

Replace item about Generic number in subclause 3.1.1.5/ETS 300 899 [11] by:

The connected number received in the connected number information element of the CONNECT message is transferred in the generic number parameter with the number qualifier indicator coded "additional connected number" without taking into account the public COLP and COLR supplementary services.

NOTE: The coding "Private numbering plan" may be used in the numbering plan indicator of the generic number parameter.

Access transport

Add the following line to table in subclause 3.1.1.5/ETS 300 899 [11] as follows:

Table A.16: Contents of the access transport parameter

←ANM	**←CONNECT**
Access transport	Content
Connected subaddress (note)	Connected subaddress
NOTE: The connected subaddress information element is transferred without taking into account the public COLP and COLR supplementary services.	

Application Transport

Table A.17: Contents of the Application Transport parameter

←ANM	←CONNECT
Application Transport	Content
Application Context Identifier "PSS1 ASE (VPN)"	
Connected number	Connected number
Facility with Protocol profile value set to "Networking Extensions"	Facility with Protocol profile value set to "Networking Extensions"
Notification indicator	Notification indicator

A.4.1.5 Sending of the Connect message (CON)

The connect message (CON) is coded as described in subclause 3.1.1.6/ETS 300 899 [11] with the following modifications.

Access transport

Add the following line to table in subclause 3.1.1.6/ETS 300 899 [11] as follows:

Table A.18: Contents of the access transport parameter

←CON	←CONNECT
Access transport	Information elements
Connected subaddress (note)	Connected subaddress
NOTE: The connected subaddress information element is transferred without taking into account the public COLP and COLR supplementary services.	

Application Transport

Table A.19: Contents of the Application Transport parameter

←CON	←CONNECT
Application Transport	Content
Application Context Identifier "PSS1 ASE (VPN)"	
VPN feature transparency indication "Call with VPN feature transparency capability" (note)	
Connected number	Connected number
Facility with Protocol profile value set to "Networking Extensions"	Facility with Protocol profile value set to "Networking Extensions"
Notification indicator	Notification indicator
NOTE: Only included if the connect message (CON) is the first backwards message sent by the destination exchange.	

Generic number

Replace item about Generic number in subclause 3.1.1.6/ETS 300 899 [11] by:

> The connected number received in the connected number information element of the CONNECT message is transferred in the generic number parameter with the number qualifier indicator coded "additional connected number" without taking into account the public COLP and COLR supplementary services.

NOTE: The coding "Private numbering plan" may be used in the numbering plan indicator of the generic number parameter.

A.4.1.6 Receipt of the Application Transport message

Upon receipt of a Application Transport message with the Application Context Identifier coded "PSS1 ASE (VPN)", the exchange transfers the following information in a FACILITY message or in a NOTIFY message.

Table A.20: Receipt of the Application Transport message

Application Transport→	**FACILITY/NOTIFY→**
Application Transport parameter	Content
Application Context Identifier "PSS1 ASE (VPN)"	
Facility	Facility
Notification indicator	Notification indicator

A.4.1.7 Sending of the Application Transport message

Upon receipt of a FACILITY message or a NOTIFY message, the exchange transfers the following information in a Application Transport message.

Table A.21: Sending of the Application Transport message

←Application Transport	**←FACILITY/NOTIFY**
Application Transport parameter	Content
Application Context Identifier "PSS1 ASE (VPN)"	
VPN feature transparency indication "Call with VPN feature transparency capability" (note)	
Facility with Protocol profile value set to "Networking Extensions"	Facility with Protocol profile value set to "Networking Extensions"
Notification indicator	Notification indicator
NOTE: Only included if the application transport message (APM) is the first backwards message sent by the destination exchange.	

A.4.1.8 Receipt of the Release message (REL)

The actions described in subclause 3.1.1.7/ETS 300 899 [11] applies with the following additions:

Upon receipt of a release message (REL) subsequent to a pre-release information message (PRI), the exchange shall transfer the following information in a DISCONNECT message.

Facility/Notification indicator

Table A.22: Receipt of the Release message

REL subsequent to a PRI message→	**DISCONNECT→**
Application Transport parameter received in the PRI message	Content
Application Context Identifier "PSS1 ASE (VPN)"	
Facility	Facility
Notification indicator	Notification indicator

A.4.1.9 Sending of the Pre-release information message (PRI)

If the call is released after the sending of the SETUP message, upon receipt of a DISCONNECT, RELEASE or RELEASE COMPLETE message, the exchange shall transfer the following information in a pre-release information message (PRI) before sending the release message.

Application Transport

Table A.23: Sending of the Pre-release information message

←PRI	**←DISCONNECT, RELEASE, RELEASE COMPLETE**
Application Transport parameter	Content
Application Context Identifier "PSS1 ASE (VPN)"	
VPN feature transparency indication "Call with VPN feature transparency capability" (note)	
Facility with Protocol profile value set to "Networking Extensions"	Facility with Protocol profile value set to "Networking Extensions"
Notification indicator	Notification indicator
NOTE: Only included if the Pre-release information message (PRI) is the first backwards message sent by the destination exchange.	

Annex B (informative): Signalling interworking specification for Transaction Capability User (TC-User)

B.1 Interworking at the Originating local exchange

B.1.1 Sending of the signalling connection establishment request

If a SETUP message coded as described in subclause "Connection-oriented bearer independent transport mechanism"/[ETS 300 196-1 [7]] is received from an access with extended DSS1 capability and if the exchange has determined that it is a VPN signalling connection requesting support of PSS1 information flows, a dialogue is established by the exchange sending a TC-BEGIN primitive with Setup invoke component with the following parameters.

CalledPartyNumber

The CalledPartyNumber parameter is generated by the VPN Application Process. This parameter is the public called party number coded as described in EN 300 356-1 [8].

VpnTransport

Table B.1: Contents of the VpnTransport parameter of the Setup invoke component

SETUP→	**TC-BEGIN→**
Content	Setup invoke VPNTransport parameter
	Business Group Identifier (note)
Non-locking shift	Non-locking shift
Transit counter	Transit counter
Calling party number	Calling party number
Called party number	Called party number
Facility with Protocol profile value set to "Networking Extensions"	Facility with Protocol profile value set to "Networking Extensions"
NOTE: The Business Group Identifier is optional. When present, it consists of two fields (BGID length and BGID, as described in clause 13) and its value is either derived from information received from the calling user in the VPN indicator information element in the SETUP message or is an implicit value tied to the incoming access.	

B.1.2 Receipt of the signalling connection establishment confirmation

Upon receipt of a TC-CONTINUE primitive with a Connect invoke component, the exchange sends a CONNECT message across the user-network interface to the calling user.

Table B.2: Sending of the CONNECT message

←CONNECT	←TC-CONTINUE
Content	Connect invoke ConnectArg parameter
Connected number	Connected number
Facility	Facility

B.1.3 Sending and receipt of private network specific information after confirmation of the signalling connection establishment

Upon receipt of a TC-CONTINUE primitive with VpnTransport invoke, the exchange transfers the following information in a FACILITY message.

Table B.3: Sending of the FACILITY message

←FACILITY	←TC-CONTINUE
Content	VpnTransport invoke VpnFacilityArg parameter
Facility	Facility

Upon receipt of a FACILITY message, the exchange shall transfer the following information in a TC-CONTINUE primitive with VpnTransport invoke.

Table B.4: Sending of the VpnTransport invoke component

FACILITY→	TC-CONTINUE→
Content	VpnTransport invoke VpnFacilityArg parameter
Facility with Protocol profile value set to "Networking Extensions"	Facility with Protocol profile value set to "Networking Extensions"

B.1.4 Release of the signalling connection

NOTE: The interworking situations where the signalling connection is released are not all described in this subclause.

B.1.4.1 Receipt of the Setup return result component

Upon receipt of a TC-END primitive with Setup return result component, the exchange transfers the following information in a RELEASE message.

Table B.5: Sending of the RELEASE message

←RELEASE	←TC-END
Content	Setup return result
Cause	Cause parameter
	Vpntransport parameter
Facility	Facility

B.1.4.2 Receipt of the Release invoke component

Upon receipt of a TC-END primitive with Release invoke component, the exchange transfers the following information in a RELEASE message.

Table B.6: Sending of the RELEASE message

←RELEASE	**←TC-END**
Content	Release invoke
Cause	Cause parameter
	Vpntransport parameter
Facility	Facility

B.1.4.3 Sending of the Release invoke component

Upon receipt of a RELEASE or RELEASE COMPLETE message, the exchange transfers the following information in a TC-END primitive with Release invoke component.

Table B.7: Sending of the Release invoke component

RELEASE, RELEASE COMPLETE→	**TC-END→**
Content	Release invoke
Cause	Cause parameter
	Vpntransport parameter
Facility with Protocol profile value set to "Networking Extensions"	Facility with Protocol profile value set to "Networking Extensions"

B.2 Interworking at the Destination local exchange

B.2.1 Sending of the SETUP message

If a TC-BEGIN primitive with Setup invoke component is received and if the called access has the extended DSS1 capability, the exchange shall send a SETUP message coded as described in subclause "Connection-oriented bearer independent transport mechanism"/(ETS 300 196-1 [7]) to the called user with the following information.

Table B.8: Sending of the SETUP message

TC-BEGIN→	SETUP→
Setup invoke VPNTransport parameter	Content
Non-locking shift	Non-locking shift
Transit counter	Transit counter
Calling party number	Calling party number
Called party number	Called party number
Facility	Facility

B.2.2 Sending of the signalling connection establishment confirmation

Upon receipt of a CONNECT message, the exchange shall send a TC-CONTINUE primitive with a Connect invoke component.

Table B.9: Sending of the Connect invoke component

←TC-CONTINUE	←CONNECT
Connect invoke ConnectArg parameter	Content
Connected number	Connected number
Facility with Protocol profile value set to "Networking Extensions"	Facility with Protocol profile value set to "Networking Extensions"

B.2.3 Sending and receipt of private network specific information after confirmation of the signalling connection establishment

Upon receipt of a TC-CONTINUE primitive with VpnTransport invoke, the exchange transfers the following information in a FACILITY message.

Table B.10: Receipt of the VpnTransport invoke component

TC-CONTINUE→	FACILITY→
VpnTransport invoke VpnFacilityArg parameter	Content
Facility	Facility

Upon receipt of a FACILITY message, the exchange transfers the following information in a TC-CONTINUE primitive with VpnTransport invoke.

Table B.11: Sending of the VpnTransport invoke component

←TC-CONTINUE	←FACILITY
VpnTransport invoke VpnFacilityArg parameter	Content
Facility with Protocol profile value set to "Networking Extensions"	Facility with Protocol profile value set to "Networking Extensions"

B.2.4 Release of the signalling connection

NOTE: The interworking situations where the signalling connection is released are not all described in this subclause.

B.2.4.1 Sending of the Release invoke component

Upon receipt of a RELEASE or RELEASE COMPLETE message, the exchange transfers the following information in a TC-END primitive with Release invoke component.

Table B.12: Sending of the Release invoke

←TC-END	←RELEASE, RELEASE COMPLETE
Release invoke	Content
Cause parameter	Cause
Vpntransport parameter	
Facility with Protocol profile value set to "Networking Extensions"	Facility with Protocol profile value set to "Networking Extensions"

B.2.4.2 Receipt of a Release invoke component

Upon receipt of a TC-END primitive with Release invoke component, the exchange shall transfer the following information in a RELEASE message.

Table B.13: Sending of the RELEASE message

TC-END→	RELEASE→
Release invoke	Content
Cause parameter	Cause
Vpntransport parameter	
Facility	Facility

History

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