INTERNATIONAL TELECOMMUNICATION UNION

# ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

# Q.765.1

(05/98)

SERIES Q: SWITCHING AND SIGNALLING

Specifications of Signalling System No. 7 – ISDN user part

# Signalling System No. 7 – Application transport mechanism – Support of VPN applications with PSS1 information flows

ITU-T Recommendation Q.765.1

(Previously CCITT Recommendation)

ITU-T Q-SERIES RECOMMENDATIONS

**SWITCHING AND SIGNALLING**

| | |
|---|---|
| SIGNALLING IN THE INTERNATIONAL MANUAL SERVICE | Q.1–Q.3 |
| INTERNATIONAL AUTOMATIC AND SEMI-AUTOMATIC WORKING | Q.4–Q.59 |
| CLAUSES APPLICABLE TO ITU-T STANDARD SYSTEMS | Q.100–Q.119 |
| SPECIFICATIONS OF SIGNALLING SYSTEMS No. 4 AND No. 5 | Q.120–Q.249 |
| SPECIFICATIONS OF SIGNALLING SYSTEM No. 6 | Q.250–Q.309 |
| SPECIFICATIONS OF SIGNALLING SYSTEM R1 | Q.310–Q.399 |
| SPECIFICATIONS OF SIGNALLING SYSTEM R2 | Q.400–Q.499 |
| DIGITAL EXCHANGES | Q.500–Q.599 |
| INTERWORKING OF SIGNALLING SYSTEMS | Q.600–Q.699 |
| SPECIFICATIONS OF SIGNALLING SYSTEM No. 7 | Q.700–Q.849 |
| General | Q.700 |
| Message transfer part (MTP) | Q.701–Q.709 |
| Signalling connection control part (SCCP) | Q.711–Q.719 |
| Telephone user part (TUP) | Q.720–Q.729 |
| ISDN supplementary services | Q.730–Q.739 |
| Data user part | Q.740–Q.749 |
| Signalling System No. 7 management | Q.750–Q.759 |
| **ISDN user part** | **Q.760–Q.769** |
| Transaction capabilities application part | Q.770–Q.779 |
| Test specification | Q.780–Q.799 |
| Q3 interface | Q.800–Q.849 |
| DIGITAL SUBSCRIBER SIGNALLING SYSTEM No. 1 | Q.850–Q.999 |
| PUBLIC LAND MOBILE NETWORK | Q.1000–Q.1099 |
| INTERWORKING WITH SATELLITE MOBILE SYSTEMS | Q.1100–Q.1199 |
| INTELLIGENT NETWORK | Q.1200–Q.1999 |
| BROADBAND ISDN | Q.2000–Q.2999 |

*For further details, please refer to ITU-T List of Recommendations.*

## ITU-T RECOMMENDATION Q.765.1

# SIGNALLING SYSTEM No. 7 – APPLICATION TRANSPORT MECHANISM – SUPPORT OF VPN APPLICATIONS WITH PSS1 INFORMATION FLOWS

### Summary

This Recommendation describes the extensions for the support of the VPN applications over the public Network Node Interface (NNI). This application makes use of the Application Transport Mechanism described in Recommendation Q.765 for bearer related signalling, and the Transaction Capability (TCAP) for signalling involving no bearer. This Recommendation specifies the respective users (i.e. APM-user, TC-user) to support the PSS1 information flows continuity in VPN applications (Transparent transfer of PSS1 information flows between PINX entities). The public NNI provides transparency to the services of the private network.

### Source

ITU-T Recommendation Q.765.1 was prepared by ITU-T Study Group 11 (1997-2000) and was approved under the WTSC Resolution No. 1 procedure on the 15th of May 1998.

### Keywords

APM, ASN.1, ISUP, PSS1, TCAP

## FOREWORD

ITU (International Telecommunication Union) is the United Nations Specialized Agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of the ITU. The ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Conference (WTSC), which meets every four years, establishes the topics for study by the ITU-T Study Groups which, in their turn, produce Recommendations on these topics.

The approval of Recommendations by the Members of the ITU-T is covered by the procedure laid down in WTSC Resolution No. 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

## NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

## INTELLECTUAL PROPERTY RIGHTS

The ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. The ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, the ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

# CONTENTS

**Page**

**Recommendation Q.765.1**

# SIGNALLING SYSTEM No. 7 – APPLICATION TRANSPORT MECHANISM – SUPPORT OF VPN APPLICATIONS WITH PSS1 INFORMATION FLOWS

*(Geneva, 1998)*

## 1 Scope

This Recommendation describes the extensions required for the support of VPN applications over the public Network Node Interface (NNI). This application makes use of the Application Transport Mechanism described in Recommendation Q.765 for bearer related signalling, and the Transaction Capability (TCAP) for signalling involving no bearer. This Recommendation specifies the respective users (i.e. APM-user, TC-user) to support the PSS1 information flows continuity in VPN applications (Transparent transfer of PSS1 information flows between PINX entities). 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 this Recommendation.

This Recommendation supports a number of network options. These are summarized in Table 1.

**Table 1/Q.765.1 – Network options**

| Option | Values | |
|---|---|---|
| Support of GFP functionality at transit PINX nodes<br>(See 6.2.5) | Full support | |
| | Partial support | Not applicable in the international network (Note 1) |
| Support of GFP functionality at gateway PINX nodes<br>(See 6.2.6) | Full support | |
| | No support | (Note 1) |
| Continuation of calls with no application association<br>(See 6.2.6) | Supported | (Note 2) |
| | Not supported | (Note 3) |
| Relocation of gateway function<br>(See 6.2.6) | Supported | |
| | 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 must be routed using a mechanism which can correctly route the call to the terminating access without use of the VPN procedures specified in this Recommendation.

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

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; all users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

[1] ISO/IEC 11574:1994, *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 11572:1997, *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 11582:1995, *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 11579-1:1994, *Information technology – Telecommunications and information exchange between systems – Private integrated services network – Part 1: Reference configuration for PISN Exchanges (PINX).*

[5] ISO/IEC 15055:1997, *Information technology – Telecommunications and information exchange between systems – Private Integrated Services Network – Specification, functional model and information flows – Transit counter additional network feature.*

[6] ISO/IEC 15056:1997, *Information technology – Telecommunications and information exchange between systems – Private Integrated Services Network – Inter-exchange signalling protocol – Transit counter additional network feature.*

[7] ITU-T Recommendation Q.711 (1993), *Signalling System No. 7 – Functional description of the signalling connection control part.*

[8] ITU-T Recommendation Q.712 (1993), *Signalling System No. 7 – Definition and function of SCCP messages.*

[9] ITU-T Recommendation Q.713 (1993), *Signalling System No. 7 – SCCP formats and codes.*

[10] ITU-T Recommendation Q.714 (1993), *Signalling System No. 7 – Signalling connection control part procedures.*

[11] ITU-T Recommendation Q.715 (1996), *Signalling connection control part user guide.*

[12] ITU-T Recommendation Q.716 (1993), *Signalling System No. 7 – Signalling Connection Control Part (SCCP) performance.*

[13] ITU-T Recommendation Q.763 (1997), *Signalling System No. 7 – ISDN User Part formats and codes.*

[14] ITU-T Recommendation Q.764 (1997), *Signalling System No. 7 – ISDN User Part signalling procedures.*

[15] CCITT Recommendation Q.767 (1991), *Application of the ISDN user part of CCITT Signalling System No. 7 for international ISDN interconnection.*

[16] ITU-T Recommendation Q.771 (1993), *Functional description of transaction capabilities.*

[17] ITU-T Recommendation Q.772 (1993), *Transaction capabilities information element definitions.*

[18] ITU-T Recommendation Q.773 (1993), *Transaction capabilities formats and codes.*

[19] ITU-T Recommendation Q.774 (1993), *Transaction capabilities procedures.*

[20] ITU-T Recommendation Q.775 (1993), *Guidelines for using transaction capabilities.*

[21] ITU-T Recommendation Q.931 (1998), *ISDN user-network interface layer 3 specification for basic call control – Annex M: Additional basic call signalling requirements for the support of private network interconnection for virtual private network applications.*

[22] ITU-T Recommendation Q.932 (1998), *Digital Subscriber Signalling System No. 1 – Generic procedures for the control of ISDN supplementary services – Annex D: Enhancements for virtual private networks.*

[23] ITU-T Recommendation Q.765 (1998), *Signalling System No. 7 – Application transport mechanism.*

[24] ITU-T Recommendation Q.1400 (1993), *Architecture framework for the development of signalling and OA&M protocols using OSI concepts.*

[25] ITU-T Recommendations X.680 to X.683 (1994), *Specification of Abstract Syntax Notation One (ASN.1).*

## 3 Definitions

Reference to PINX functionality within this Recommendation refers to "virtual PINX" functionality implemented on the public NNI.

Within the scope of this Recommendation, "VPN" refers to a Virtual Private Network with the support of PSS1 information flows.

## 4 Abbreviations

This Recommendation uses the following abbreviations.

| | |
|---|---|
| ACM | Address Complete Message |
| AE | Application Entity |
| AEI | Application Entity Invocation |
| ALS | Application Layer Structure |
| ANM | Answer Message |
| AP | Application Process |
| APM | Application Transport Mechanism |
| APM-user | Application Transport Mechanism User Application |
| APP | Application Transport Parameter |
| ASE | Application Service Element |
| CLIP | Calling Line Identification Presentation |
| CLIR | Calling Line Identification Restriction |
| CNID | Corporate Telecommunications Network Identifier |

| | |
|---|---|
| COLP | Connected Line Identification Presentation |
| COLR | Connected Line Identification Restriction |
| CON | Connect Message |
| COPSS1 | Connection Oriented PSS1 |
| CPG | Call Progress Message |
| DPINX | Destination PINX |
| GFP | Generic Functional Protocol |
| IAM | Initial Address Message |
| IN | Intelligent Network |
| 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 |
| PAN | Public Addressed Node |
| PIN | Public Initiating Node |
| PINX | Private Integrated Services Network Exchange |
| PRI | Pre-Release Information Message |
| PSS1 | Private Network Q Reference Point Signalling System No. 1 |
| 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 |
| TC | Transaction Capabilities |
| TE | Transit Exchange |
| TPINX | Transit PINX |
| UCEH | Unidentified Context and Error Handling |

| | |
|---|---|
| UNI | User-Network Interface |
| VPN | Virtual Private Network |

## 5 Recommendation structure

The description of the ISDN User Part and the TC-user procedures in this Recommendation are structured according to the model described in 6.2. 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".

This Recommendation 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 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 APM [23]. For signalling requiring no bearer, it describes the services provided by 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 coordinated by the Single Association Coordination Function (SACF).

The Connection Oriented signalling association without a bearer is subdivided into two parts: Connection Oriented PSS1 (COPSS1 ASE), and Transaction Capability (TC ASE). These are coordinated by the Single Association Coordination Function (SACF).

The Application Process (AP) contains all Call Control functions; however, this Recommendation will only describe the enhancements required to support VPN applications. The Application Process relevant to private network functionality can be found in other Recommendations (reference [1] and reference [2]), as can that for the public ISUP basic call [14].

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 must 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 reference [13])/operation structure (as specified in this Recommendation) and in the proper sequence (as specified in reference [14] and this Recommendation).

The structure and examples of its usage are illustrated diagrammatically in 6.2.

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 6.1. The APM ASE provides the 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.

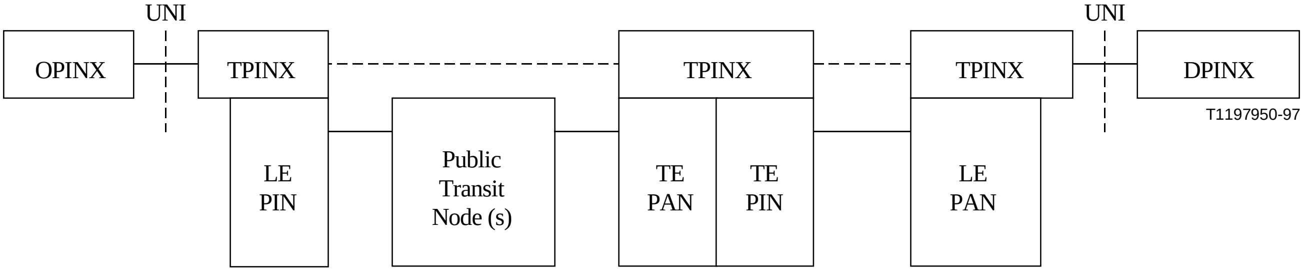
The private network specifications (reference [1]) make a reference to specific private network primitives between Call Control and Protocol Control representing the PSS1 information flows. The Application Process in this Recommendation describes the relationship between these primitives and how they relate to the suitable primitives in the ALS model for the transport of the PSS1 information flows.

Examples of the bearer unrelated signalling mechanism can be found in 11.1.

## 6 Modelling

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

### 6.1 Network model



**Network model**

**Figure 1/Q.765.1 – 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 reference [23] 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 Public Initiating Node (PIN) and the Public Addressed Node (PAN). The PAN identifies the particular APM-user application by the Context Identifier value carried within the Application Transport Parameter (APP), in this case "PSS1 ASE (VPN)". The PAN identifies the particular PINX application related to a specific corporate network identified by a Corporate Telecommunications Network Identity (e.g. CNID 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 dependent 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 routing 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.

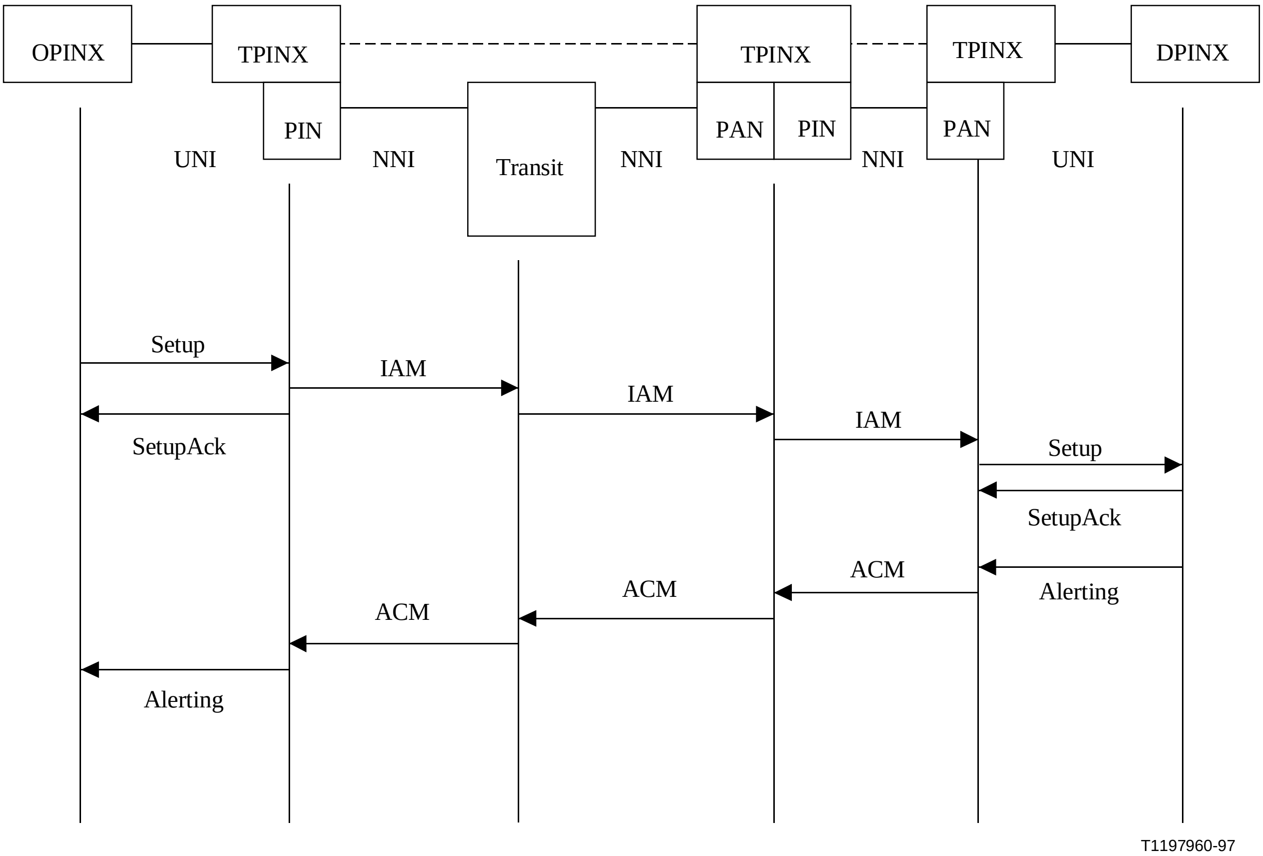


**Figure 2/Q.765.1 – One example of a message sequence for call with bearer**

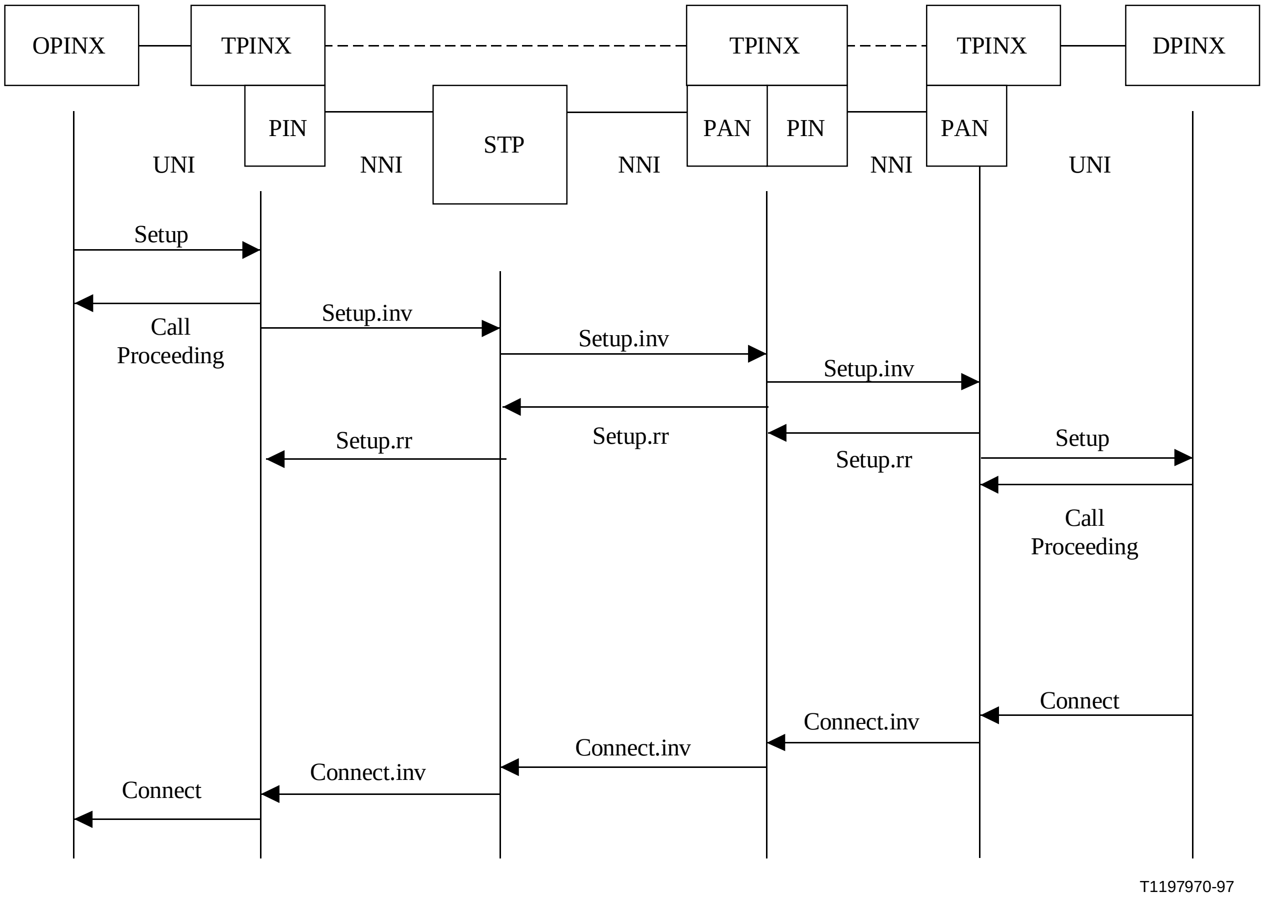


**Figure 3/Q.765.1 – One example of an operation sequence for call without a bearer**

## 6.2 Specification model

### 6.2.1 Introduction

The model used to structure the description of ISUP and TC-USER application procedures is based on the OSI Application Layer Structure (ALS) model (see reference [24]). This subclause presents the model, gives a general description of its operation and shows the generalized model for the "Exchange Application Process" for the support of PSS1 information flows in virtual private networks and in VPN application for the support of PSS1 information flows over the public Network Node Interface (NNI). It shows how the application makes use of the Application Transport Mechanism (APM) which is described in detail in reference [23].

### 6.2.2 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 below. Figure 4 shows the primitive interfaces between the functional blocks, as used in the body of this Recommendation 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 nodal functions (AP) and the SACF for the support of PSS1 information flows in VPN applications over the NNI: see 7.2.2.

(b) Interface to PSS1 ASE which defines the formats and codes in the APP for the support of PSS1 information flows in VPN applications: see 10.1.

(c) Interface between SACF and UCEH ASE representing the handling of unidentified context identifier values and error cases associated with the Application Transport mechanism: reference [23].

(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 out of the scope of this Recommendation): reference [23].

(e) Interface to public ISUP basic call signalling ASE : (this interface is out of the scope of this Recommendation): reference [23].

(f) Interface between SACF and NI function: (this interface is out of the scope of this Recommendation): reference [23].

(g) Interface to MTP-3: (this interface is out of the scope of this Recommendation): reference [23].

(h) Interface between TC SACF and AP: see 7.3.2.

(i) Interface between TC SACF and COPSS1 ASE which performs the function of the protocol control for bearer unrelated Connection Oriented signalling: see 11.1.

(j) Interface between TC SACF and TC ASE which provides the services defined in reference [16]: see 12.1.

(k) Interface between TC SACF and SCCP which provides the services defined in reference [7]: see 13.1.

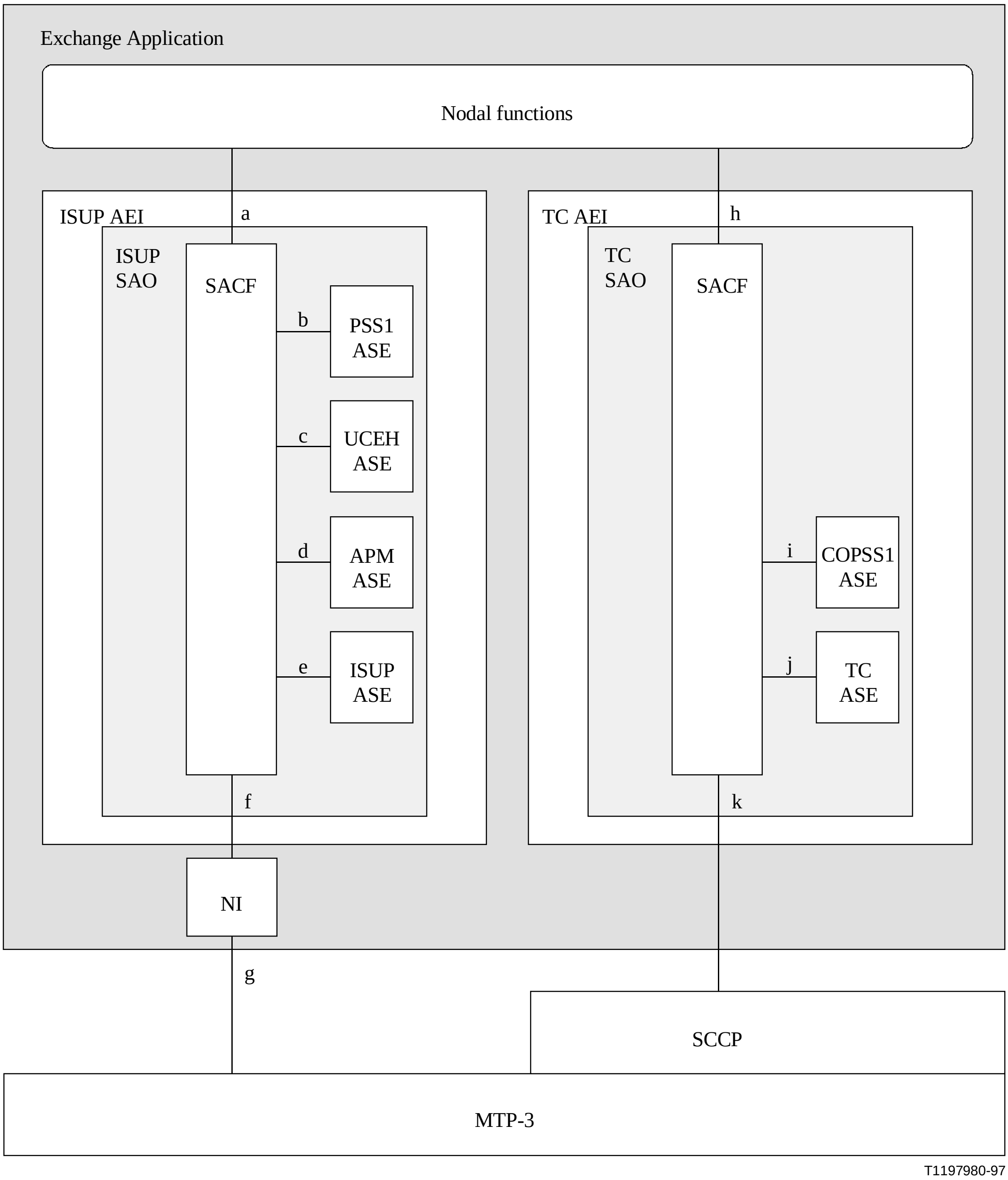


**Figure 4/Q.765.1 – ISUP and Connection Oriented signalling specification model**

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 this Recommendation. 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 this Recommendation.

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

The SACF has the responsibility of coordinating the flow of primitives between its interfaces in the appropriate manner.

The ISUP ASE is defined by reference [14]. Its main responsibilities are basic call procedures and the handling of protocol errors and unrecognized information handling. The monolithic nature of these Recommendations means that both Public Call Control and Protocol Control functionality are defined together. It is not the intention of this Recommendation to redefine reference [14] in ALS format, therefore it is referenced *en bloc* within this Recommendation 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 outside the scope of this Recommendation. (See reference [23].)

The APM ASE provides the means for the transfer of information between nodes for signalling requiring a bearer, and provides 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 2048 octets of application information. The APM ASE is able to support multiple APM-users where each is treated independently and provided with the same level of service. It consists of two distinct sets of functions: one set used as the Public Addressed Node (PAN) and one set used as the Public Initiating Node (PIN) (supporting the signalling association towards to PAN). The PIN/PAN concept is explained in 6.1/Q.765 [23].

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 reference [23].) 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 Transport 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 references [16] to [20].

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 Public Addressed Node (PAN) and Public Initiating Node (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 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 SSN and the TC dialogue ID. The NI is described in detail in reference [23].

The SCCP interface is described in references [7] to [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.

### 6.2.3 Dynamic primitive flows

#### 6.2.3.1 Bearer related signalling flows

Figures 5 and 6 illustrate the dynamic primitive flows for a VPN call with PSS1 information flow support being supported over the NNI (ISUP) for the case that 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.

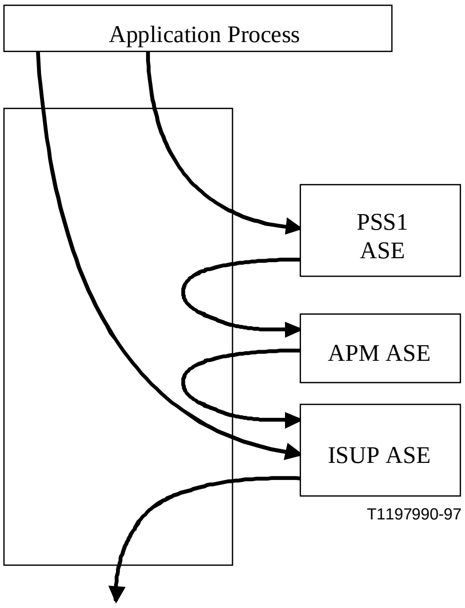


**Figure 5/Q.765.1**

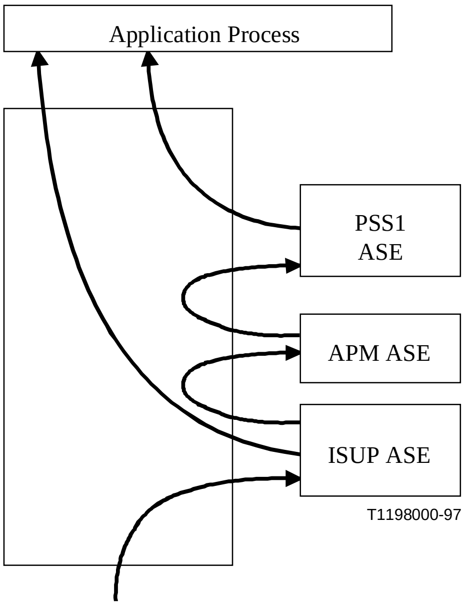


**Figure 6/Q.765.1**

Figures 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 coincidentally. 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.

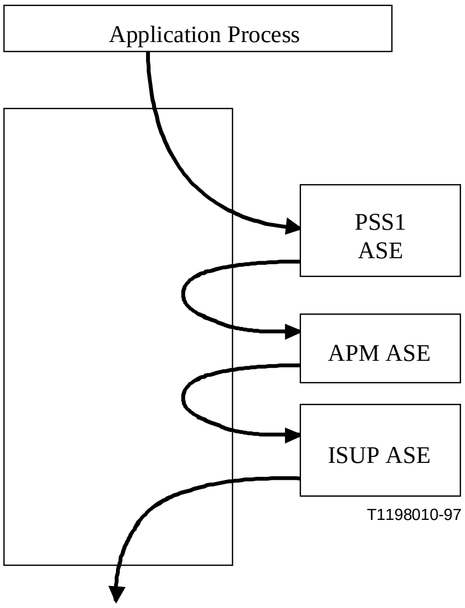


**Figure 7/Q.765.1**

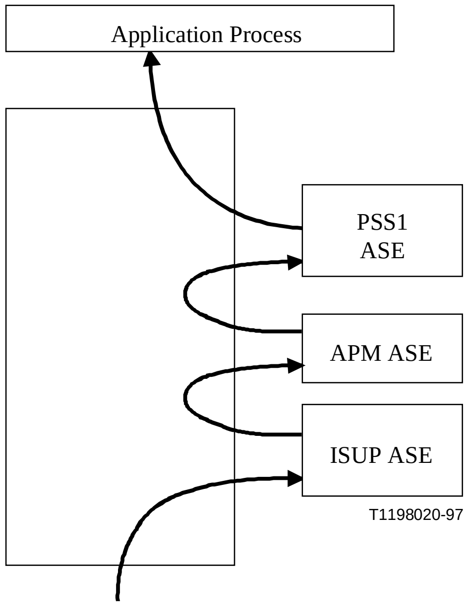


**Figure 8/Q.765.1**

### 6.2.3.2 Bearer unrelated signalling flows

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

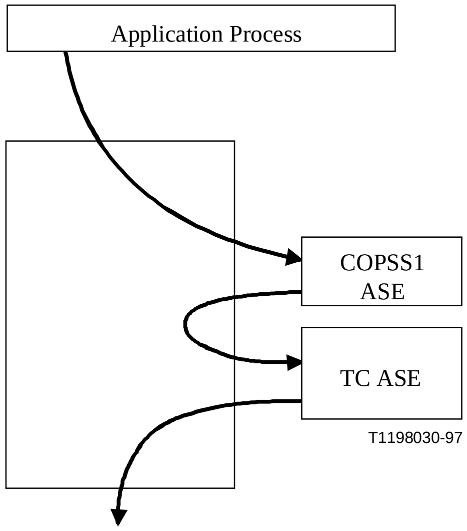


**Figure 9/Q.765.1**

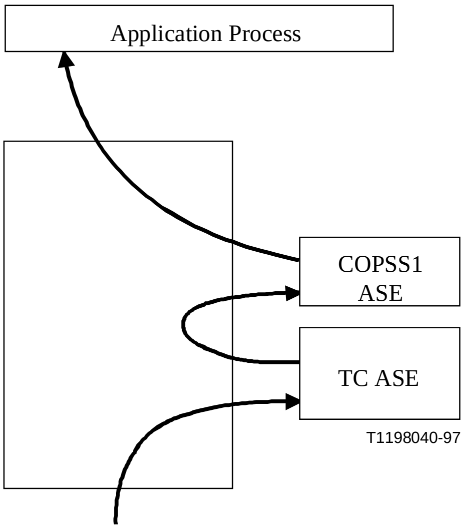


**Figure 10/Q.765.1**

### 6.2.4 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 fall-back situation occurs inside the VPN (i.e. a loss of PSS1 information flows continuity) then 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.

### 6.2.5 Transit PINX function – Generic functional protocol

Two cases must 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 (reference [3]), which includes analysis of the 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 VPN node would pass on PSS1-GF information received in a Facility information element, with the protocol profile set to "networking extensions", transparently between two PINXs that are directly connected to the VPN.

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 must be used and supported and the use of option 2 can be agreed to be supported across the international interface through bilateral agreements between network operators.

### 6.2.6 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 (see 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 7.2.3.2.5).

NOTE – This includes the situation where the PAN is the DLE 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.

In the case 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-operators 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 must 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 two 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.

# 7 Application Process functions

## 7.1 General

The modelling of the Application Process (AP) is outside the scope of this Recommendation; however, in order to appreciate the role of the AP for the purposes of this Recommendation, 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 reference [23] and ISUP basic call [14]) and the Virtual Private

Network (VPN) applications for the support of PSS1 functionality, as defined in this Recommendation.

The aspect of the Application Process that this Recommendation introduces is the required coordination between the public 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 6.2.4, 6.2.5 and 6.2.6. In order to show the relationship between the VPN AP and the PSS1 Call Control logic, this Recommendation defines the mapping between the Call Control/Protocol Control [2] and the SACF interface (a) primitives. It also describes the additional VPN specific procedures. The description of either the public or PINX Application Processes are outside the scope of this Recommendation.

The definition of the primitive interface at the Application Process/SACF for the public Application Transport Mechanism is outside the scope of this Recommendation.

## 7.2 VPN Application Process functions – Connection with call (bearer related)

### 7.2.1 Introduction

The function of the Public NNI support of VPN applications aspect of the Application Process (AP) is to coordinate between the private network (PSS1) Application Process and the public Application Process functionality. When the private application requires to establish a signalling association with a bearer, the AP converts the private address information into the form that the public Application Process can use for routing the call from the Public Initiating Node (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 reference [23]. The specific private network use of the concept is described in 6.1. Details of the Public basic call routing information requirements can be found in reference [14]. The conversion of private information to a form suitable for routing through the public network is outside the scope of this Recommendation. It is network specific as to how the appropriate public routing 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 this Recommendation to redefine the PSS1 PINX functionality, therefore the call control defined in reference [1] applies. The purpose of this Recommendation 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 reference [2]) are fulfilled in a VPN, thus achieving PSS1 information flow continuity over the public NNI.

It is the responsibility of the VPN Application Process to ensure that the public basic call and PSS1 Call Control states remain aligned.

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

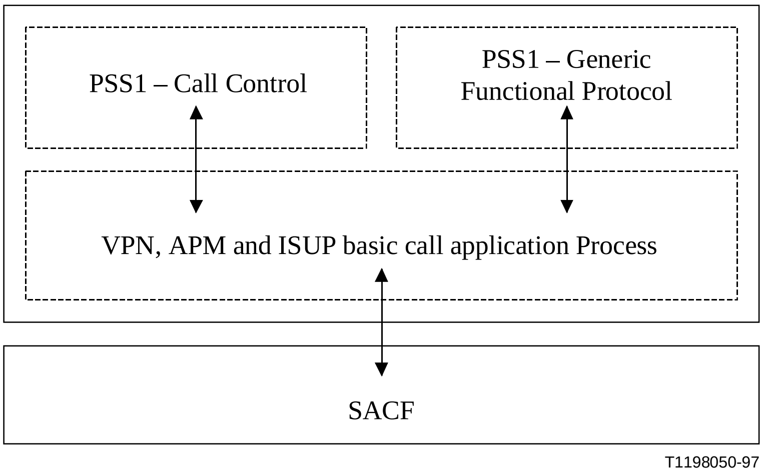

PSS1 – Call Control
PSS1 – Generic Functional Protocol
VPN, APM and ISUP basic call application Process
SACF
T1198050-97

**Figure 11/Q.765.1 – 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 coexist 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 Corporate Telecommunications Network Identifier (CNID) 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 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 6.2.6. This signalling capability may not be fulfilled if the call is routed through nodes such as a Q.767 ISUP [15], a public gateway node or a non-ISUP protocol. To cater for the case when the intermediate nodes and their associated signalling capabilities cannot support the transport of PSS1 information flows using the Application Transport Mechanism, 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" (VTI) indication] and to inform the preceding PINX that Gateway PINX functionality is required to be invoked. The mechanism to have the Gateway function invoked must 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 must 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 must 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.

### 7.2.2 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 Virtual Private Network (VPN) functionality. The primitives related to the public network functionality are outside the scope of this Recommendation, although references are made to them through functional inferences within the text. The public basic call Recommendation 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 this Recommendation. See Table 2.

**Table 2/Q.765.1 – Primitives between AP and ISUP SACF (Virtual Private Network Support)**

| Primitive name | Types | Direction (Note) |
|---|---|---|
| PSS1_Data | Indication/Request | ➔/🡐 |
| PSS1_Error | Indication | ➔ |
| Remote_Status | Indication | ➔ |
| NOTE – Primitive flow from SACF to AP: ➔<br>Primitive flow from AP to SACF: 🡐 | | |

### 7.2.3 Procedures

#### 7.2.3.1 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 references [1] and [2], and the Generic functional protocol for the support of supplementary services Standard [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/Q.765.1 – Mapping between PSS1 primitives defined in reference [2] and AP/ISUP SACF primitives**

| Primitives to/from CC Interface (reference [2]) | | Flow | 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_INFORMATION | REQ | → | APM/ACM | +PSS1_DATA.Req |
| | IND | ← | APM/ACM/CPG | +PSS1_DATA.Ind |
| PC_INFORMATION | REQ | → | APM | +PSS1_DATA.Req |
| | IND | ← | APM | +PSS1_DATA.Ind |
| 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/Q.765.1 – Mapping between PSS1 primitives defined in reference [5] and AP/ISUP SACF primitives**

| Primitives to/from CC Interface (reference [5]) | | Flow | 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/Q.765.1 – Mapping between PSS1 primitives defined in reference [3] and AP/ISUP SACF primitives**

| Primitives to/from CC Interface (reference [3]) | | Flow | ISUP Messages | Primitives to/from AP/SACF Interface (PSS1 ASE) |
|---|---|---|---|---|
| PC_DATA | REQ | → | IAM/ACM/ANM/CON/CPG/PRI/APM | +PSS1_DATA.Req |
| | IND | ← | IAM/ACM/ANM/CON/CPG/PRI/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 |

#### 7.2.3.2 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 coexist in the public network environment.

##### 7.2.3.2.1 Handling of address information

**Procedures at the PIN**

The called party number sent in the PSS1_Data request primitive sent at call establishment is also, as a national option, 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, as a national option, 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 are 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 are 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 is transferred without taking into account the public COLP and COLR supplementary services in the primitive corresponding to the CON or ANM message.

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

##### 7.2.3.2.2 Corporate Telecommunications Network Identifier

The Corporate Telecommunications Network Identifier (CNID) is either supplied over the incoming User-Network Interface (UNI) access, or it has an implicit value tied to the incoming access. The CNID 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 Corporate Telecommunications Network within their own domain. On receipt of a CNID that is not recognized by the PAN, then the call shall be released with cause 63 (service or option not available – unspecified) and the management function notified.

##### 7.2.3.2.3 Application Transport Instruction Indicators

The Application Transport Instruction Indicators (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 the call. Alternatively if actions are required to be performed to gracefully handle the case that the communication is not successful but the call is to continue, then 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.

### 7.2.3.2.4 Acknowledgement from peer application (Overlap sending)

**Procedures at the PAN**

On reception of the PC_More_Information.Request primitive, the AP will send a PSS1_Data.request primitive indicating "Setup Acknowledgement" causing an APM message to be sent towards the PIN.

**Procedures at the PIN**

On reception of the PSS1_Data.indication primitive indicating "Setup Acknowledgement", the AP will send PC_More_Information.Indication primitive. The PIN shall send the remainder of the private Called party number digits (if any) in the Called party number parameter of one or more PSS1_Data Request primitives resulting in one or more APM messages. The Sending Complete parameter may also be sent according to the PSS1 Call Control overlap procedures.

### 7.2.3.2.5 Subsequent node does not support APM/VPN

**Procedures at the PAN**

When a call is being established with PSS1 feature transparency capability, it implicitly requests 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 6.2.6:

- In the case that 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 a subsequent node.
- On reception of a notification that the peer APM user was not present at the PAN [APP parameter with Application Context Identifier field coded "Unidentified Context and Error Handling (UCEH) ASE" and with the Application Transport Notification information coded "PSS1 ASE (VPN)" (APM-user Context Identifier field) and "unidentified context" (Reason field), received in an ACM, CON, ANM, CPG, APM or PRI message].
- On receipt of the primitive corresponding to the CON message without any APP parameter coded "PSS1 ASE (VPN)" (ACI field) and a previous message with the indication of "call with VPN feature transparency capability" has not been received.
- On receipt of the primitive corresponding to the ANM message without any APP parameter coded "PSS1 ASE (VPN)" (ACI field) and a previous message with the indication of "call with VPN feature transparency capability" has not been received.

- 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.
- On receipt of the primitive corresponding to the ACM message indicating "subscriber free", without any APP parameter coded "PSS1 ASE (VPN)" (ACI field) and a previous message with the indication of "call with VPN feature transparency capability" has not been received.
- On receipt of the primitive corresponding to the CPG message indicating "Alerting", without any APP parameter coded "PSS1 ASE (VPN)" (ACI field) and a previous message with the indication of "call with VPN feature transparency capability" has not been received.

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, the call shall be released with cause 63 (service or option not available – unspecified) and the management function notified.

#### 7.2.3.2.6 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 must be taken into account when using this feature.

Receipt of the "Gateway PINX Transformation Request" indication takes precedence over the procedures described in 7.2.3.2.5 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 to transform 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 7.2.3.2.5 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 indicates 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 to transform 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 6.2.6).

It shall then, as a network option, check the note in memory to determine if a previous node has the capability to transform 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".

### 7.2.3.4 Relay node

The Relay node functionality distinguishes VPN calls, and relays 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 to establish a signalling association with a bearer, the AP generates public routing information in the form that the public Application Process can use for routing the call from the Public Initiating Node (PIN) to the appropriate exchange in the public network, Public Addressed Node (PAN), which contains the PINX functionality. Details of the Public basic call routing information requirements can be found in reference [14]. The public routing information is implicitly tied to the particular Corporate Telecommunications Network Identifier associated with the access.

The Relay node performs the interworking of PSS1 information flows between the User-Network Interface (UNI) and the Network Node Interface (NNI) protocols. The private network specific information is passed transparently and distributed to primitives on the AP/ISUP SACF interface in the same manner as if the information was received from the private call control logic, hence the private network specific information flow transparency is achieved.

The Relay node can be considered as illustrated in Figure 12.

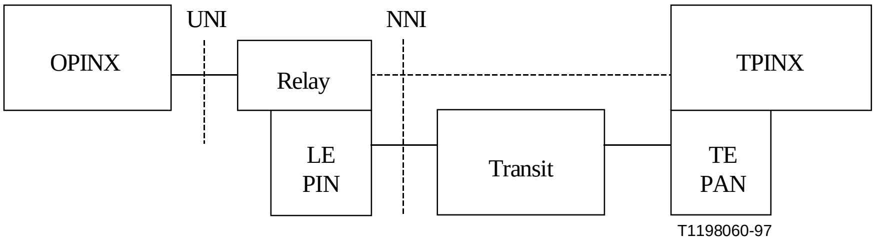


**Figure 12/Q.765.1 – Illustration of a Relay node interworking the UNI and NNI protocols thereby interfacing between two PINX functions**

### 7.2.4 Exceptional procedures

### 7.2.5 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 6.2.6) then the node shall invoke gateway PINX functionality (see 7.2.3.2.5). 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 will be allowed to proceed if possible, else the call shall be released.

On reception of a PSS1_Error indication primitive containing an error notification indicating "unrecognized mandatory information", the call shall be released with cause code 111 – Protocol error, unspecified.

### 7.2.6 Primitive contents

Tables 6 and 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/Q.765.1 – Contents of the PSS1_Data Ind/Req primitive**

| Parameter | Mandatory/Optional |
|---|---|
| ATII | M |
| VPN feature transparency indication | O |
| Gateway PINX transformation capability | O |
| CNID | O |
| Gateway PINX request | O |
| SetupAcknowledgment | O |
| Calling party number | O |
| Called party number | O |
| Connected number | O |
| Facility (Note) | O |
| Notification indicator (Note) | O |
| Sending Complete | O |
| Transit counter | O |
| NOTE – These parameters may be repeated. | |

**Table 7/Q.765.1 – Contents of the PSS1_Error Ind primitive**

| Parameter | Mandatory/Optional |
|---|---|
| Error Notification | M |

**Table 8/Q.765.1 – 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 | • Called party number (M)<br>• ATII (M)<br>• Gateway PINX transformation capability (O)<br>• CNID (O)<br>• Calling party number (O)<br>• Facility (O) (Note)<br>• Notification indicator (O) (Note)<br>• Sending Complete (O)<br>• Transit counter (O) |
| ACM | • ATII (M)<br>• VPN feature transparency indication (O)<br>• Facility (O) (Note)<br>• Notification indicator (O) (Note) |
| CPG | • ATII (M)<br>• VPN feature transparency indication (O)<br>• Facility (O) (Note)<br>• Notification indicator (O) (Note) |
| ANM | • ATII (M)<br>• VPN feature transparency indication (O)<br>• Connected number (O)<br>• Facility (O) (Note)<br>• Notification indicator (O) (Note) |
| CON | • ATII (M)<br>• VPN feature transparency indication (O)<br>• Connected number (O)<br>• Facility (O) (Note)<br>• Notification indicator (O) (Note) |
| PRI | • ATII (M)<br>• VPN feature transparency indication (O)<br>• Facility (O) (Note)<br>• Notification indicator (O) (Note) |
| APM | • ATII (M)<br>• Called party number (O)<br>• SetupAcknowledgement (O)<br>• VPN feature transparency indication (O)<br>• Facility (O) (Note)<br>• Notification indicator (O) (Note)<br>• Sending Complete (O) |
| NOTE – These parameters may be repeated. | |

## 7.3 VPN Application Process functions – Connection without call (bearer unrelated)

### 7.3.1 Introduction

The function of the Public NNI support of VPN applications aspect of the Application Process (AP) is to coordinate between the private network (VPN) Application Process and the public Application Process functionality. When the private application requires to establish a signalling association without a bearer, the AP converts the private address information into the form that the public Application Process can use for routing from the Public Initiating Node (PIN) to the appropriate node in the public network, Public Addressed Node (PAN), which contains the adjacent PINX functionality. The PIN/PAN concept is described in reference [23]. The specific private network use of the concept is described in 3.1. The conversion of private information to a form suitable for routing through the public network is outside the scope of this Recommendation.

It is not the intention of this Recommendation to redefine the PSS1 PINX functionality. The purpose of this Recommendation is to describe how, through the use of TC and SCCP, the services expected by PSS1 at the Generic Functional Transport (GFT) /Protocol Control (PC) interface (defined in reference [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/IEC model in reference [3]) is not seen on any interface in the ALS. It is not the intention of this Recommendation to model the AP; however, to illustrate the relationship between this Recommendation and the PINX functionality defined by ISO, Figure 11 can be used.

Connectionless signalling is not supported by this Recommendation.

### 7.3.2 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/Q.765.1 – Primitives between AP and TC SACF**

| Primitive name | Types | Direction (Note) |
|---|---|---|
| PSS1_Setup | Indication/Request/Response/Confirmation | →/←/←/→ |
| PSS1_Release | Indication/Request | →/← |
| PSS1_Reject | Indication/Request | →/← |
| PSS1_Facility | Indication/Request | →/← |
| PSS1_SetupAck | Indication/Request | →/← |
| NOTE – Primitive flow from SACF to AP: →<br>Primitive flow from AP to SACF: ← | | |

### 7.3.3 Connection Oriented signalling procedures

The protocol control procedures that describe the mapping of the Generic Functional Transport (GFT) primitives to transaction (TC) operations over the public NNI are described here with reference to reference [3]. The procedural aspects of the PINX functionality are outside the scope of this Recommendation (see 6.2.5 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, this Recommendation defines the mapping between the primitives referred to in reference [3] and the suitable AP/TC SACF interface primitives. See Table 10.

Primitives related to the private application functionality are outside the scope of this Recommendation (see reference [3]).

**Table 10/Q.765.1 – Mapping between primitives used in reference [3] and AP/TC SACF primitives**

| COLUMN A<br>Primitives used at GFT/PC interface<br>as defined in reference [3] | COLUMN B<br>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 |

#### 7.3.3.1 Corporate Telecommunications Network Identifier

The Corporate Telecommunications Network Identifier (CNID) is either supplied over the incoming User-Network Interface (UNI) access, or it has an implicit value tied to the incoming access. The CNID is only required for call establishment [SETUP operation (TC)] 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 Corporate Telecommunications Network within their own domain. On receipt of a (CNID) that is not recognized by the PAN, the connection shall then be released with cause 63 (service or option not available – unspecified) and the management function notified.

#### 7.3.3.2 Relay node

See 7.2.3.4.

### 7.3.4 Primitive contents

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

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/Q.765.1 – Contents of the PSS1_SETUP Ind/Req**

| Parameter | Mandatory/Optional |
|---|---|
| Public Called Party Number | M |
| Called Party Number | M |
| Calling Party Number | O |
| Corporate Telecommunications Network Identifier | O |
| Facility (Note) | O |
| Transit Counter | O |
| NOTE – These parameters may be repeated. | |

**Table 12/Q.765.1 – Contents of the PSS1_SETUP Res/Conf primitive**

| Parameter | Mandatory/Optional |
|---|---|
| Connected Number | O |
| Facility (Note) | O |
| NOTE – These parameters may be repeated. | |

**Table 13/Q.765.1 – Contents of the PSS1_RELEASE Ind/Req primitive**

| Parameter | Mandatory/Optional |
|---|---|
| Cause | M |
| Facility (Note) | O |
| NOTE – These parameters may be repeated. | |

**Table 14/Q.765.1 – Contents of the PSS1_REJECT Ind/Req primitive**

| Parameter | Mandatory/Optional |
|---|---|
| Cause | M |
| Facility (Note) | O |
| NOTE – These parameters may be repeated. | |

**Table 15/Q.765.1 – Contents of the PSS1_FACILITY Ind/Req primitive**

| Parameter | Mandatory/Optional |
|---|---|
| Facility (Note) | M |
| NOTE – These parameters may be repeated. | |

## 8 Single Association Control Function (SACF) – ISUP SACF

### 8.1 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) in Figure 4] towards NI [interface (f) in Figure 4] or vice versa, therefore the SACF is also responsible to ensure that when multiple primitives are generated by the ASEs towards the AP, that they are delivered across the interface together to ensure 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 outside the scope of this Recommendation. The mapping of primitives in Tables 16 and 19 are in reference [23] and are included here for informative purposes only.

The interfaces referenced herein are illustrated in 6.2, Figure 4. Examples of the "Dynamic primitive flows" can be found in 6.2.3.

The primitives on the interface between SACF and the AP, interface (a), are defined in 7.2.2.

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

The primitives on the interface between SACF and PSS1 ASE, interface (b), are defined in 10.1.

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 reference [23] and are therefore outside the scope of this Recommendation.

The primitives on the interface between SACF and APM ASE, interface (d), can be found in reference [23] and are therefore outside the scope of this Recommendation.

The primitives on the interface between SACF and ISUP ASE, interface (e), can be found in reference [23] and are therefore outside the scope of this Recommendation.

The primitives on the interface between SACF and NI, interface (f), can be found in reference [23] and are therefore outside the scope of this Recommendation.

### 8.2 Information flows related to messages sent by the node

On receipt of a primitive (request or response) from the Application Process (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/Q.765.1 – Mapping between PSS1 ASE and APM ASE primitives**

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

**Table 17/Q.765.1 – Mapping between AP and PSS1 ASE primitives**

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

### 8.3 Information flows related to messages received by the node

These procedures are described in reference [23] where the APM-user ASE corresponds with the PSS1 ASE.

**Table 18/Q.765.1 – 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/Q.765.1 – Mapping between APM ASE and PSS1 ASE primitives**

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

**Table 20/Q.765.1 – Mapping between UCEH ASE and PSS1 ASE primitives**

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

## 9 Single Association Control Function (SACF) – TC SACF

### 9.1 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 this Recommendation:

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

The interfaces referenced herein are illustrated in 6.2, Figure 4. Subclause 6.2.3 also provides examples of the "Dynamic primitive flows".

The primitives received from the AP, on interface h), are mapped as shown in 7.3.2 and 7.4.2. The parameters in these primitives are listed in 7.3.5.

The primitives on the interface between SACF and COPSS1 ASE, interface (i), are listed in 11.1.

The primitives on the interface between SACF and TCAP, interface (j), are listed in references [16] to [20]. (See clause 12.)

The primitives on the interface between SACF and SCCP, interface (k), are listed in references [7] to [12]. (See clause 13.)

### 9.2 Information flows related to operations sent by the node

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. See Table 21.

**Table 21/Q.765.1 – 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 |

### 9.3 Information flows related to operations received by the node

On receipt of a N_DATA indication primitive from the SCCP, the SACF analyses the User Data field of this primitive according to the rules in reference [9]. It then proceeds to perform the function of distribution. See Table 22.

**Table 22/Q.765.1 – 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 |

## 10 PSS1 ASE (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.

### 10.1 Primitive interface

Table 23 lists the primitive interface between the PSS1 ASE and ISUP SACF, [interface (b) in Figure 4].

**Table 23/Q.765.1 – Primitives between ISUP SACF and PSS1 ASE (APM)**

| Primitive name | Types | Direction (Note) |
|---|---|---|
| APM_U_Data | Indication/Request | →/← |
| APM_U_Error | Indication | → |
| PSS1_Error | Indication | → |
| PSS1_Data | Indication/Request | →/← |
| NOTE – Primitive flow from SACF to PSS1 ASE: →<br>Primitive flow from PSS1 ASE to SACF: ← | | |

### 10.2 Signalling procedures

#### 10.2.1 Public Initiating Node

##### 10.2.1.1 Sending procedures

On reception of the PSS1_Data.request primitive, its contents are prepared in the appropriate format (see clause 14) and the context identifier value set to "PSS1 ASE (VPN)". The result is sent in the APM_U_Data.request primitive.

#### 10.2.1.2 Receiving procedures

On reception of the APM_U_Data.indication primitive, its contents are checked for correct format and coding (see clause 14). If the check is passed, the received information is transferred and sent in the PSS1_Data.indication primitive. If the check is failed, then also send the PSS1_Error.indication primitive with the results and indicating "unrecognized information". If an unrecognized value is received for the CNID indicator field, then the Error Notification sent in the PSS1_Error indication primitive shall indicate "unrecognized mandatory information".

#### 10.2.1.3 APM_U_Error Primitive

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

### 10.2.2 Public Addressed Node

See 10.2.1.

### 10.2.3 Signalling congestion

In order to avoid congestion in the No. 7 signalling network, it is necessary that applications that contribute signalling load towards a congested destination limit their signalling traffic in a controlled manner. As the AP makes use of the ISUP ASE, the ISDN User Part signalling congestion control procedure [14] may reduce traffic towards an affected destination. As such new call attempts may temporarily be rejected.

## 10.3 Primitive contents

Tables 24 and 25 list the mandatory and optional contents for the PSS1 ASE service primitives. These primitives are defined in reference [23] 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 7.2.6

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

**Table 24/Q.765.1 – 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/Q.765.1 – Contents of the APM_U_Error Ind primitive**

| Parameter | Mandatory/Optional |
|---|---|
| Notification | M |

## 11 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.

### 11.1 TC-user sequence

**Signalling flow for call setup and cleardown**

In Figure 13, 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 are 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, VpnFacility***. The Setup operation is of class 3 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 sending the Setup return result operation. Both timers are restarted on sending/receipt of an operation.

A class 3 operation called ***ActivityTest*** is 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 T1, T2 or T4, the PIN shall send a TC-U-ABORT (abort the dialogue) and inform the management function.

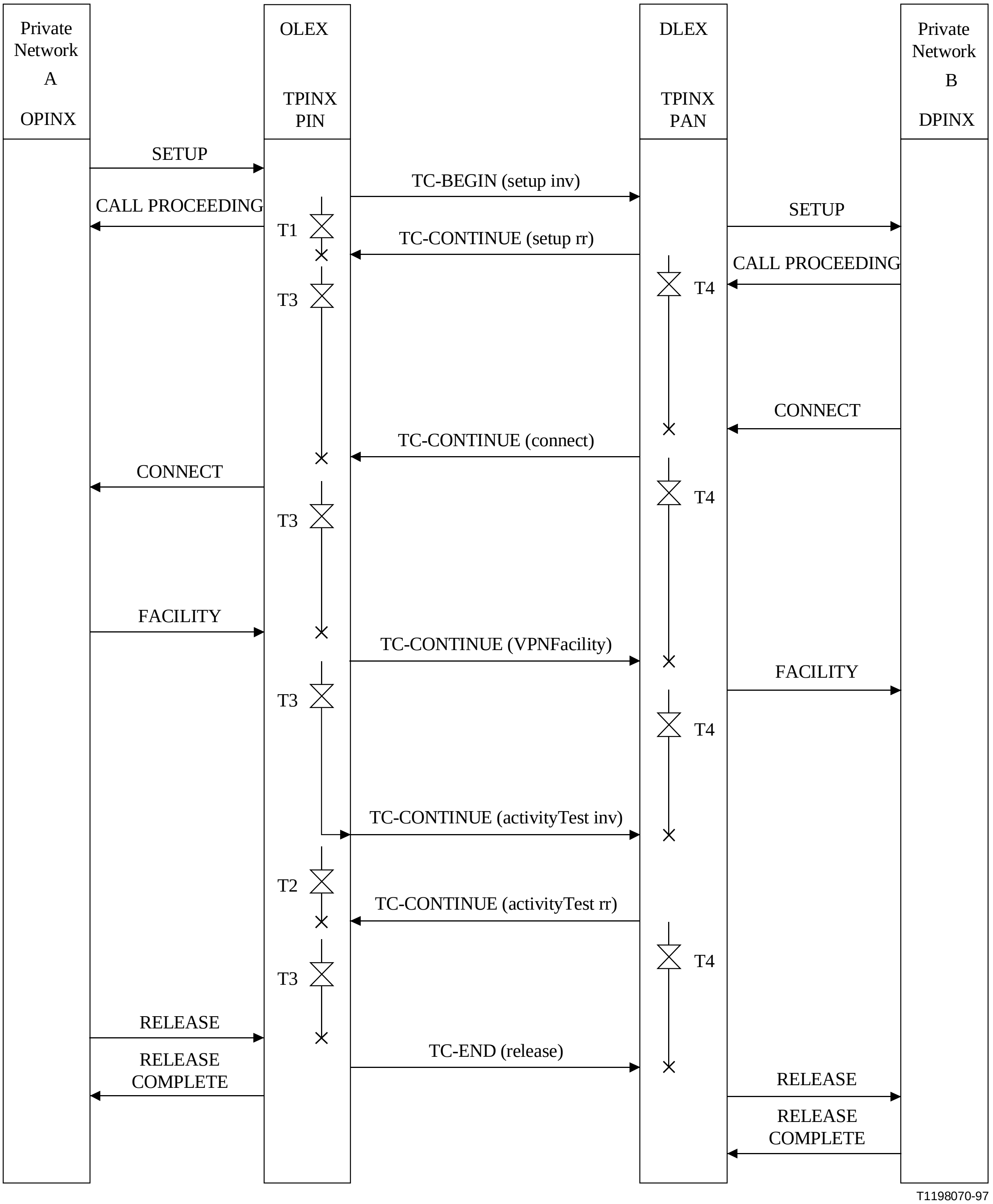


**Figure 13/Q.765.1 – Example of a bearer unrelated signalling sequence**

## 11.2 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 references [16] and [17].

**Table 26/Q.765.1 – Primitives between COPSS1-ASE and TC SACF (Protocol Control)**

| Primitive name | Types | Direction (Note) | 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 | ➔/🡐 | VpnFacility.Invoke |
| PSS1_RELEASE | Indication/Request | ➔/🡐 | Release.Invoke |
| NOTE – Primitive flow from SACF to COPSS1 ASE: ➔<br>Primitive flow from COPSS1 ASE to SACF: 🡐 | | | |

### 11.3 Supported operations

The ASE supports the following Operations:

| | |
|---|---|
| • Setup | (Class 3). |
| • Connect | (Class 4). |
| • VpnFacility | (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
- VpnFacility
  - VpnFacility.Invoke
- Release
  - Release.Invoke
- ActivityTest
  - ActivityTest.Invoke
  - ActivityTest.ReturnResult

### 11.4 ASE procedures

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

#### 11.4.1 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, is done by TC.

All the operations below belong to the same dialogue.

Class 3 and 4 operations are used.

Each TC message conveys only a single operation.

##### 11.4.1.1 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 shall be included in this case. In addition, one or more Facility "Networking extensions" information elements may be included in the VPNTransport parameter.

##### 11.4.1.2 Dialogue continuing

The continuation of the dialogue is assumed by the Connect (class 4), VpnFacility (class 4) and ActivityTest (class 3) operations using TC-CONTINUE primitives.

##### 11.4.1.3 Dialogue end

###### 11.4.1.3.1 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.

###### 11.4.1.3.2 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.

#### 11.4.2 Operations

##### 11.4.2.1 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.

#### 11.4.2.2 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.

#### 11.4.2.3 VpnFacility operation

The VpnFacility 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 VpnFacility.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 VpnFacility.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.

#### 11.4.2.4 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.

#### 11.4.2.5 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.

#### 11.4.2.6 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".

### 11.4.3 Expiry of timers

#### 11.4.3.1 T1

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

#### 11.4.3.2 T2

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

#### 11.4.3.3 T3

On expiry of timer T3, the activity test procedures shall be initiated (see 11.4.2.4).

#### 11.4.3.4 T4

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

### 11.4.4 Signalling congestion

In order to avoid congestion in the No. 7 signalling network, it is necessary that applications that contribute signalling load towards a congested destination limit their signalling traffic in a controlled manner. As the AP makes use of the TC ASE, the COPSS1 ASE shall take appropriate action on receipt of a TC-NOTICE primitive indicating signalling congestion. Similar to the procedures for the ISDN User Part signalling congestion control [14], the AP should reduce the establishment of new transactions towards the affected destination.

## 11.5 Primitive contents

The contents of the primitives are described in 7.3.4.

## 11.6 Abstract syntax, general

Subclause 11.8 specifies the abstract syntax for the COPSS1 ASE protocol using the Abstract Syntax Notation One (ASN.1) [25].

The set of values each of which is a value of the ASN.1 type TCAPMessages, MessageType as defined in references [16] to [20] with the ANY DEFINED BY definitions resolved by the operations and errors definitions included in 11.8 form the abstract syntax for the COPSS1 ASE protocol.

The set of encoding rules which are applicable to this abstract syntax are defined by references [16] to [20]. The mapping of the OPERATION and ERROR MACROs to TC components is also described in references [16] to [20].

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".

### 11.7 Subsystem number

The SSN value of 0000 1011 "ISDN supplementary services" will be used.

### 11.8 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 reference [25] and using the OPERATION and ERROR macros as defined by references [16] to [20].

The formal definition of the component types to encode these operations, errors and types is provided in references [16] to [20].

```
COPSS1 -Protocol {itu-t Recommendation q 765 1 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:      3

--Timer:      T1

--Purpose:    Used for the establishment of a signalling association between a PIN and a PAN for a bearer unrelated
signalling connection.


SetUp         ::= OPERATION

          ARGUMENT

              SetUpArg

          RESULT

              SetUpResultArg


--Specification of Connect

-- =================

--Direction:  DLEX → OLEX

--Class:      4
```

*--Purpose: Indicates that the signalling connection has reached the active state.*

**Connect ::= OPERATION**

**ARGUMENT**

**ConnectArg**

*--Specification of Release*

-- ==================

*--Direction: OLEX → DLEX and DLEX → OLEX*

*--Class: 4*

*--Purpose: Used for releasing a signalling association between a PIN and a PAN.*

**Release ::= OPERATION**

**ARGUMENT**

**ReleaseArg**

*--Specification of VpnFacility*

**-- ===================**

*--Direction: OLEX → DLEX and DLEX → OLEX*

*--Class: 4*

*--Purpose: Used for transporting PSS1 information flows during the active phase of a signalling connection.*

**VpnFacility ::= OPERATION**

**ARGUMENT**

**VpnFacilityArg**

*--Specification of ActivityTest*

-- =====================

*--Direction: OLEX → DLEX*

*--Class: 3*

*--Timer: T2*

*--Purpose: Used to determine if the signalling association remains established between a PIN and a PAN.*

**ActivityTest ::= OPERATION**

```
            RESULT


================================================================================
--TYPE DEFINITIONS FOR ERRORS
================================================================================

-
================================================================================
-- TYPE DEFINITIONS FOR ARGUMENT DATA
================================================================================

SetUpArg                ::= SEQUENCE {

        calledPartyNumber                   CalledPartyNumber,

        vpntransport                  VPNTransport,

        ...

        }


SetUpResultArg          ::= SEQUENCE {

        cause                         [0] Cause OPTIONAL,

        vpntransport                  [1] VPNTransport OPTIONAL,

        ...

        }


ConnectArg              ::= VPNTransport


ReleaseArg              ::= SEQUENCE {

        cause                         Cause,
        vpntransport                  [0] VPNTransport OPTIONAL,
        ...
        }
VpnFacilityArg          ::= VPNTransport
================================================================================
--TYPE DEFINITIONS FOR DATA
================================================================================
CalledPartyNumber       ::= OCTET STRING (SIZE (1..maxcdPlength))
        --The CalledPartyNumber is coded as described in Recommendation Q.763 [13].
        --The ISUP parameter name and length octets are not included.

VPNTransport            ::= OCTET STRING (SIZE (0..maxLength))
        --The VPNTransport is coded as described in clause 14/Q.765.1.

Cause                   ::= OCTET STRING (SIZE (1..maxCauseLength))
        --The Cause is coded as described in ISO/IEC 11572 [2]/ Q.931 Annex M [21]
        --The information element identifier and length octets are not included.
```

```
==================================================================================
--DEFINITION OF RANGE CONSTANTS
==================================================================================
maxCauseLength              INTEGER         ::= 30
maxLength                   INTEGER         ::= 2048
maxcdPlength                INTEGER         ::= Network specific
==================================================================================
--DEFINITION OF OBJECT IDENTIFIER PATH
==================================================================================
COPSS1OID       OBJECT IDENTIFIER    ::= {itu-t Recommendation q 765 1 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
```

## 12 TCAP (TC ASE)

The SACF uses the services provided by the TCAP primitive interface. The definition of TCAP is outside the scope of this Recommendation. For details refer to references [16] to [20].

### 12.1 Interface TCAP/SACF

#### 12.1.1 Primitives

The primitives at this interface that support the services offered by TCAP are defined in references [16] to [20].

#### 12.1.2 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.

## 13 SCCP

### 13.1 Interface SCCP/SACF

The TC-SACF uses the services provided by the SCCP primitive interface. The definition of SCCP is outside the scope of this Recommendation. For details refer to the SCCP references [7] to [12].

### 13.2 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 1992 version of SCCP to be used, but preferably 1996/97 version of SCCP [7] to [12] to be used.

### 13.3 Routing in the SCCP network

For routing on the international interface and for routing 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) |
| Routing indicator | 0 | (Routing on global title) |

Alternatively, for routing 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 SS No. 7 routing data manageable.

### 13.4 Number information used for routing

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 routing 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.

## 14 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 (see 14.1) as well as having the ability of passing additional network related information (see 14.2) 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 14.1). 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 14.2) to be passed between VPN applications residing within the public network.

### 14.1 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/Q.765.1 – Information elements transported within the APP**

| Information Element | Ref. | Type | Length |
|---|---|---|---|
| Calling party number | [2]/[21] (Note 1) | O | 4-* |
| Called party number | [2]/[21] (Note 1) | O | 4-* |
| Connected number | [2]/[21] (Note 1) | O | 4-* |
| Facility with protocol profile value set to "Networking extensions" (Note 2) | [3]/[22] (Note 1) | O | 3-* |
| Notification indicator (Note 2) | [3]/[22] (Note 1) | O | 3-* |
| Locking Shift | [3]/[21] (Note 1) | O | 1 |
| Non-locking Shift | [3]/[21] (Note 1) | O | 1 |
| Sending Complete | [2]/[21] (Note 1) | O | 1 |
| Transit counter | [6]/[21] (Note 1) | O | 3 |

NOTE 1 – The definition of these information elements by ISO/IEC [2]/[3]/[6] and by ITU-T [21]/[22] are identical and therefore equally applicable.

NOTE 2 – These information elements may be repeated.

NOTE 3 – The information elements carried in the Application Transport Parameter are taken into account whatever the order of receipt is with the exception of the Locking and Non-locking shift information elements which operate in the specific way.

### 14.2 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 | CNID indicator | | SAI | GR | GT | VTI |
| 2 | CNID length | | | | | | | |
| 3<br>:<br>14 | CNID | | | | | | | |

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 (SAI)

| | |
|---|---|
| 0 | No indication |
| 1 | Setup acknowledgement |

e) Corporate Telecommunications Network Identifier Indicator (CNID indicator)

| | | |
|---|---|---|
| 00 | Not included | (Network option) |
| 01 | Network specific | (Network option) |
| 10 | Global Value | |
| 11 | Spare | |

f) Extension indicator (Ext)

| | |
|---|---|
| 0 | Information continues through the next octet |
| 1 | Last octet |

g) Corporate Telecommunications Network Identifier length (CNID length)

Number of octets containing CNID

When the CNID indicator is coded 00 "Not included", then CNID length is omitted

h) Corporate Telecommunications Network Identifier (CNID)

Binary value

When the CNID indicator is coded 00 "Not included", octets 3-14 are omitted.

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

## 15 Timers

This clause specifies all the Application Process and Protocol timers relevant for VPN applications. For each timer the time-out 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.

## 15.1 Timers in TC-user

See Table 28.

**Table 28/Q.765.1 – Timers in TC-user**

| Symbol | Time-out value | Cause for initiation | Normal termination | At expiry | Reference |
|---|---|---|---|---|---|
| T1 | 1-5 sec | Sending of SETUP.Invoke | Reception of SETUP.ReturnResult | Abort dialogue<br>Send TC-U-ABORT<br>Inform management function | 11.4.3.1 |
| T2 | 1-5 sec | Sending of ActivityTest.invoke | Reception of ActivityTest.ReturnResult | Abort dialogue<br>Send TC-U-ABORT<br>Inform management function | 11.4.3.2 |
| T3 | 10-60 min | Reception of<br>Setup.ReturnResult<br>Connect.Invoke<br>VPNFacility.Invoke<br>ActivityTest.ReturnResult<br>Sending of VPNFacility.Invoke | Reception of<br>Connect.Invoke<br>VPNFacility.Invoke<br>Release.Invoke<br>Sending of ActivityTest.Invoke | Send ActivityTest.Invoke | 11.4.3.3 |
| T4 | 10-60 min<br>(Note T4 must be greater than T3) | Reception of VPNFacility.Invoke<br>Sending of<br>Setup.ReturnResult<br>Connect.Invoke<br>VPNFacility.Invoke<br>ActivityTest.ReturnResult | Reception of ActivityTest.Invoke<br>Sending of<br>Connect.Invoke<br>VPNFacility.Invoke<br>Release.Invoke | Abort dialogue<br>Send TC-U-ABORT<br>Inform management function | 11.4.3.4 |

# ITU-T RECOMMENDATIONS SERIES

| | |
|---|---|
| Series A | Organization of the work of the ITU-T |
| Series B | Means of expression: definitions, symbols, classification |
| Series C | General telecommunication statistics |
| Series D | General tariff principles |
| Series E | Overall network operation, telephone service, service operation and human factors |
| Series F | Non-telephone telecommunication services |
| Series G | Transmission systems and media, digital systems and networks |
| Series H | Audiovisual and multimedia systems |
| Series I | Integrated services digital network |
| Series J | Transmission of television, sound programme and other multimedia signals |
| Series K | Protection against interference |
| Series L | Construction, installation and protection of cables and other elements of outside plant |
| Series M | TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits |
| Series N | Maintenance: international sound programme and television transmission circuits |
| Series O | Specifications of measuring equipment |
| Series P | Telephone transmission quality, telephone installations, local line networks |
| **Series Q** | **Switching and signalling** |
| Series R | Telegraph transmission |
| Series S | Telegraph services terminal equipment |
| Series T | Terminals for telematic services |
| Series U | Telegraph switching |
| Series V | Data communication over the telephone network |
| Series X | Data networks and open system communications |
| Series Y | Global information infrastructure |
| Series Z | Programming languages |