UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T Q.765.1

(05/98)

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

SÉRIE Q: COMMUTATION ET SIGNALISATION

Spécifications du système de signalisation n° 7 – Sous-système utilisateur du RNIS

Système de signalisation n° 7 – Mécanisme de transport d'application: Prise en charge des applications de réseau privé virtuel avec les flux informationnels du système PSS1

Recommandation UIT-T Q.765.1

(Antérieurement Recommandation du CCITT)

RECOMMANDATIONS UIT-T DE LA SÉRIE Q

COMMUTATION ET SIGNALISATION

SIGNALISATION DANS LE SERVICE MANUEL INTERNATIONAL	Q.1–Q.3
EXPLOITATION INTERNATIONALE AUTOMATIQUE ET SEMI-AUTOMATIQUE	Q.4–Q.59
FONCTIONS ET FLUX D'INFORMATION DES SERVICES DU RNIS	Q.60–Q.99
CLAUSES APPLICABLES AUX SYSTÈMES NORMALISÉS DE L'UIT-T	Q.100–Q.119
SPÉCIFICATIONS DES SYSTÈMES DE SIGNALISATION N° 4 ET N° 5	Q.120–Q.249
SPÉCIFICATIONS DU SYSTÈME DE SIGNALISATION N° 6	Q.250–Q.309
SPÉCIFICATIONS DU SYSTÈME DE SIGNALISATION R1	Q.310–Q.399
SPÉCIFICATIONS DU SYSTÈME DE SIGNALISATION R2	Q.400–Q.499
COMMUTATEURS NUMÉRIQUES	Q.500–Q.599
INTERFONCTIONNEMENT DES SYSTÈMES DE SIGNALISATION	Q.600–Q.699
SPÉCIFICATIONS DU SYSTÈME DE SIGNALISATION N° 7	Q.700–Q.849
Généralités	Q.700
Sous-système transport de messages	Q.701–Q.709
Sous-système commande des connexions sémaphores	Q.711–Q.719
Sous-système utilisateur de téléphonie	Q.720–Q.729
Services complémentaires du RNIS	Q.730–Q.739
Sous-système utilisateur de données	Q.740–Q.749
Gestion du système de signalisation n° 7	Q.750–Q.759
Sous-système utilisateur du RNIS	**Q.760–Q.769**
Sous-système application de gestion des transactions	Q.770–Q.779
Spécification des tests	Q.780–Q.799
Interface Q3	Q.800–Q.849
SYSTÈME DE SIGNALISATION D'ABONNÉ NUMÉRIQUE N° 1	Q.850–Q.999
RÉSEAUX MOBILES TERRESTRES PUBLICS	Q.1000–Q.1099
INTERFONCTIONNEMENT AVEC LES SYSTÈMES MOBILES À SATELLITES	Q.1100–Q.1199
RÉSEAU INTELLIGENT	Q.1200–Q.1999
RNIS À LARGE BANDE	Q.2000–Q.2999

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

RECOMMANDATION UIT-T Q.765.1

SYSTEME DE SIGNALISATION N° 7 – MECANISME DE TRANSPORT D'APPLICATION: PRISE EN CHARGE DES APPLICATIONS DE RESEAU PRIVE VIRTUEL AVEC LES FLUX INFORMATIONNELS DU SYSTEME PSS1

Résumé

La présente Recommandation décrit les compléments nécessaires pour la prise en charge d'applications de réseau privé virtuel (VPN) de part et d'autre de l'interface nodale avec le réseau (NNI, *network node interface*). Cette application fait usage du mécanisme de transport d'application qui est décrit dans la Recommandation Q.765 pour la signalisation relative aux circuits supports ainsi qu'au sous-système application pour la gestion des transactions (TCAP, *transaction capability*) pour la signalisation non relative à un circuit support. La présente Recommandation spécifie les utilisateurs respectifs (c'est-à-dire l'utilisateur APM et l'utilisateur-TC) pour prendre en charge la continuité des flux informationnels du système PSS1 dans les applications VPN (transfert transparent de flux informationnels PSS1 entre entités de commutateur PINX). L'interface NNI avec le réseau public assure la transparence avec les services du réseau privé.

Source

La Recommandation UIT-T Q.765.1, élaborée par la Commission d'études 11 (1997-2000) de l'UIT-T, a été approuvée le 15 mai 1998 selon la procédure définie dans la Résolution n° 1 de la CMNT.

Mots clés

APM, ASN.1, ISUP, PSS1, TCAP

AVANT-PROPOS

L'UIT (Union internationale des télécommunications) est une institution spécialisée des Nations Unies dans le domaine des télécommunications. L'UIT-T (Secteur de la normalisation des télécommunications) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

La Conférence mondiale de normalisation des télécommunications (CMNT), qui se réunit tous les quatre ans, détermine les thèmes d'études à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution n° 1 de la CMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un Membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux responsables de la mise en œuvre de consulter la base de données des brevets du TSB.

TABLE DES MATIÈRES

Page

Recommandation Q.765.1

SYSTEME DE SIGNALISATION N° 7 – MECANISME DE TRANSPORT D'APPLICATION: PRISE EN CHARGE DES APPLICATIONS DE RESEAU PRIVE VIRTUEL AVEC LES FLUX INFORMATIONNELS DU SYSTEME PSS1

(Genève, 1998)

1 Domaine d'application

La présente Recommandation décrit les compléments nécessaires pour la prise en charge d'applications de réseau privé virtuel (VPN) de part et d'autre de l'interface nodale avec le réseau (NNI). Cette application fait usage du mécanisme de transport d'application qui est décrit dans la Recommandation Q.765 pour la signalisation relative aux circuits supports ainsi qu'au sous-système application pour la gestion des transactions (TCAP) pour la signalisation non relative à un circuit support. La présente Recommandation spécifie les utilisateurs respectifs (c'est-à-dire l'utilisateur APM et l'utilisateur TC) pour prendre en charge la continuité des flux informationnels du système PSS1 dans les applications VPN (transfert transparent de flux informationnels PSS1 entre entités de commutateur PINX). L'interface NNI avec le réseau public assure la transparence avec les services du réseau privé.

La capacité de réseau privé est définie par l'ISO dans sa série de normes relatives au réseau privé à intégration de services. La présente Recommandation introduit par ailleurs le concept de "nœud relais".

La présente Recommandation prend en charge un certain nombre d'options de réseau, qui sont résumées dans le Tableau 1 ci-dessous.

Tableau 1/Q.765.1 – Options de réseau

Option	Valeurs	
Prise en charge de la capacité de protocole GFP aux nœuds PINX de transit (voir 6.2.5)	Prise en charge complète	
	Prise en charge partielle	Non applicable dans le réseau international (Note 1)
Prise en charge de la capacité de protocole GFP aux nœuds PINX de passerelle (voir 6.2.6)	Prise en charge complète	
	Pas de prise en charge	(Note 1)
Continuation des communications sans association d'application (voir 6.2.6)	Option prise en charge	(Note 2)
	Option non prise en charge	(Note 3)

Tableau 1/Q.765.1 – Options de réseau *(fin)*

Option	Valeurs	
Déplacement de la fonction de passerelle (voir 6.2.6)	Option prise en charge	
	Option non prise en charge	
NOTE 1 – L'utilisation de ces options peut avoir pour résultat que certains services complémentaires de réseau privé ont un comportement inattendu ou ne fonctionnent pas du tout. NOTE 2 – Dans ce cas, les communications par VPN doivent pouvoir être acheminées correctement jusqu'à l'accès terminal sans utilisation des procédures VPN spécifiées dans la présente Recommandation. NOTE 3 – Dans ce cas, il est requis que les procédures VPN ne soient utilisées que pour des communications acheminées vers des adresses connues comme prenant en charge l'application VPN via une signalisation acceptant le mécanisme APM; sinon, la communication sera libérée.		

2 Références normatives

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui de ce fait en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée.

[1] ISO/CEI 11574:1994, *Technologies de l'information – Télécommunications et échange d'information entre systèmes – Réseau privé avec intégration de services – Services porteurs sur 8 kilo-octets par seconde en mode circuit – Description du service, aptitudes fonctionnelles et courants d'information*.

[2] ISO/CEI 11572:1997, *Technologies de l'information – Télécommunications et échange d'information entre systèmes – Réseau privé avec intégration de services – Services porteurs en mode circuit – Procédures et protocoles de signalisation d'interéchange.*

[3] ISO/CEI 11582:1995, *Technologies de l'information – Télécommunications et échange d'informations entre systèmes – Réseau privé à intégration de services – Protocole générique fonctionnel pour le support de compléments de service – Procédures et protocole de signalisation entre commutateurs.*

[4] ISO/CEI 11579-1:1994, *Technologies de l'information – Télécommunications et échange d'information entre systèmes – Réseau privé avec intégration de services – Partie 1: configuration de référence pour échanges de PISN (PINX).*

[5] ISO/CEI 15055:1997, *Technologies de l'information – Télécommunications et échange d'information entre systèmes – Réseau privé à intégration de services – Spécification, modèle fonctionnel et flux d'informations – Facilité de réseau additionnelle de compteur de transfert.*

[6] ISO/CEI 15056:1997, *Technologies de l'information – Télécommunications et échange d'information entre systèmes – Réseau privé à intégration de services – Protocole de signalisation d'interéchange – Facilité de réseau additionnelle du réseau de compteur de transfert.*

[7] Recommandation UIT-T Q.711 (1993), *Système de signalisation n° 7 – Description fonctionnelle du sous-système commande des connexions sémaphores.*

[8] Recommandation UIT-T Q.712 (1993), *Système de signalisation n° 7 – Définition et fonction des messages du sous-système commande des connexions sémaphores.*

[9] Recommandation UIT-T Q.713 (1993), *Système de signalisation n° 7 – Formats et codes du sous-système commande des connexions sémaphores.*

[10] Recommandation UIT-T Q.714 (1993), *Système de signalisation n° 7 – Procédures du sous-système commande des connexions sémaphores.*

[11] Recommandation UIT-T Q.715 (1996), *Guide d'utilisation du sous-système commande des connexions sémaphores.*

[12] Recommandation UIT-T Q.716 (1993), *Fonctionnement attendu du sous-système commande des connexions sémaphores.*

[13] Recommandation UIT-T Q.763 (1997), *Système de signalisation n° 7 – Formats et codes du sous-système utilisateur pour le RNIS.*

[14] Recommandation UIT-T Q.764 (1997), *Système de signalisation n° 7 – Procédures de signalisation du sous-système utilisateur du RNIS*.

[15] Recommandation Q.767 du CCITT (1991), *Application du sous-système utilisateur du RNIS du système de signalisation n° 7 du CCITT pour les interconnexions RNIS internationales*.

[16] Recommandation UIT-T Q.771 (1993), *Description fonctionnelle du gestionnaire de transactions*.

[17] Recommandation UIT-T Q.772 (1993), *Définition des éléments d'information du gestionnaire de transactions*.

[18] Recommandation UIT-T Q.773 (1993), *Formats et codes du gestionnaire de transactions*.

[19] Recommandation UIT-T Q.774 (1993), *Procédures du gestionnaire de transactions*.

[20] Recommandation UIT-T Q.775 (1993), *Guide d'utilisation du gestionnaire de transactions*.

[21] Recommandation UIT-T Q.931 (1998), *Spécification de la couche 3 de l'interface usager-réseau RNIS pour la commande de l'appel de base. Annexe M: Prescriptions additionnelles de signalisation d'appel de base pour la prise en charge des interconnexions avec des réseaux privés pour des applications de réseau privé virtuel.*

[22] Recommandation UIT-T Q.932 (1998), *Système de signalisation d'abonné numérique n° 1 – Procédures génériques pour la commande des services complémentaires RNIS – Annexe D: Extensions pour réseaux privés virtuels.*

[23] Recommandation UIT-T Q.765 (1998), *Mécanisme de transport d'application*.

[24] Recommandation UIT-T Q.1400 (1993), *Cadre architectural d'élaboration des protocoles de signalisation et d'exploitation, administration et maintenance utilisant les concepts de l'interconnexion de systèmes ouverts.*

[25] Recommandations X.680 à X.683 du CCITT (1994), *Notation de syntaxe abstraite numéro un (ASN.1).*

3 Définitions

Dans le cadre de la présente Recommandation, une capacité de "nœud PINX" désigne une capacité de "nœud PINX virtuel" implémentée à l'interface NNI avec le réseau public.

Dans le cadre de la présente Recommandation, l'abréviation "VPN" se rapporte à un réseau privé virtuel prenant en charge les flux informationnels du système PSS1.

4 Abréviations

La présente Recommandation utilise les abréviations suivantes:

ACM message d'adresse complète (*address complete message*)

AE entité d'application (*application entity*)

AEI invocation d'entité d'application (*application entity invocation*)

ALS structure de la couche Application (*application layer structure*)

ANM message de réponse (*answer message*)

AP processus d'application (*application process*)

APM mécanisme de transport d'application (*application transport mechanism*)

APM-user utilisateur du mécanisme APM (*application transport mechanism user application*)

APP paramètre de transport d'application (*application transport parameter*)

ASE élément de service d'application (*application service element*)

CL commutateur local

CLIP identification de la ligne appelante (*calling line identification presentation*)

CLIR restriction d'identification de la ligne appelante (*calling line presentation restriction*)

CNID identificateur de réseau de télécommunication d'entreprise (*corporate telecommunications network identifier*)

COLP identification de la ligne connectée (*connected line identification presentation*)

COLR restriction d'identification de la ligne connectée (*connected line identification restriction*)

CON message de connexion (*connect message*)

COPSS1 système PSS1 en mode connexion (*connection oriented PSS1*)

CPG message de progression d'appel (*call progress message*)

CT commutateur de transit

DPINX commutateur PINX de destination (*destination PINX*)

GFP protocole fonctionnel générique (*generic functional protocol*)

IAM message initial d'adresse (*initial address message*)

ISUP sous-système utilisateur pour le RNIS (*ISND user part*)

M/O obligatoire/facultatif (*mandatory/optional*)

MACF fonction de contrôle à associations multiples (*multiple association control function*)

MTP-3 sous-système transport de messages (*message transfer part*)

NFE extension d'élément de réseau (*network facility extension*)

NI interface avec le réseau (*network interface*)

NNI interface nodale avec le réseau (*network node interface*)

OPINX commutateur PINX d'origine (*originating PINX*)

PAN nœud public adressé (*public addressed node*)

PIN nœud public initiateur (*public initiating node*)

PINX commutateur de réseau privé à intégration de services (*private integrated services network exchange*)

PRG message de progression d'appel (*call progress message*)

PRI message d'information avant libération (*pre-release information message*)

PSS1 système de signalisation n° 1 au point de référence Q d'un réseau privé (*private network Q référence point signalling system No. 1*)

PTS point de transfert sémaphore

REL message de libération (*release message*)

RI réseau intelligent

RNIS réseau numérique à intégration de services

SACF fonction de contrôle d'association unique (*single association control function*)

SAO objet d'association unique (*single association object*)

SCCP sous-système commande des connexions sémaphores (*signalling connection control part*)

SDL langage de description et de spécification (*specification and description language*)

SID identificateur de signalisation (*signalling identifier*)

SIO octet de service (*service indicator octet*)

SSN numéro de sous-système (*subsystem number*)

TC sous-système gestionnaire de transactions (*transaction capabilities*)

TPINX commutateur PINX de transit (*transit PINX*)

UCEH traitement de non-identification de contexte et d'erreur (*unidentified context and error handling*)

UNI interface usager-réseau (*user-network interface*)

VPN réseau privé virtuel (*virtual private network*)

5 Structure de la Recommandation

La description du sous-système ISUP et les procédures d'utilisateur du sous-système TC sont, dans la présente Recommandation, structurées conformément au modèle décrit au 6.2. La description sera donc divisée en deux parties comme suit:

- fonctions protocolaires;
- fonctions non protocolaires, c'est-à-dire fonctions nodales de commutateur, appelées "processus d'application".

La présente Recommandation ne décrit, dans l'ensemble des fonctions de commutation (protocolaires et de processus d'application), que celles qui se rapportent aux extensions d'interface NNI pour prendre en charge l'interconnexion des réseaux privés pour des applications VPN.

Les fonctions protocolaires sont subdivisées en deux domaines: les associations sémaphores avec support (ISUP) et les associations sémaphores sans support (utilisateur TC en mode connexion). Pour les communications avec support, la présente Recommandation décrit l'utilisation des services fournis par le mécanisme APM [23]. Pour la signalisation sans support, la présente Recommandation décrit les services fournis par le sous-système TCAP.

L'association sémaphore avec support est subdivisée en trois parties: le protocole d'applications du système PSS1 (élément PSS1 ASE), le mécanisme de transport d'application (élément APM ASE) et l'appel de base ISUP (élément ISUP ASE). Ces trois éléments sont coordonnés par la fonction de contrôle d'association unique (SACF).

L'association sémaphore en mode connexion sans support est subdivisée en deux parties: le système PSS1 en mode connexion (élément COPSS1 ASE) et le gestionnaire de transactions (élément TC ASE). Ces deux éléments sont coordonnés par la fonction de contrôle d'association unique (SACF).

Le processus d'application (AP) contient toutes les fonctions de commande d'appel, mais la présente Recommandation ne décrit que les extensions requises pour prendre en charge les applications VPN. Le processus d'application concernant la fonction de réseau privé est décrit dans d'autres Recommandations (références [1] et [2]), de même que l'appel public de base ISUP ([14]).

La technique des primitives de service est utilisée pour définir les éléments ASE et la fonction SACF propre aux besoins sémaphores de l'application. Elle constitue un moyen pour décrire la façon dont les services offerts par un élément ASE, ou par une fonction SACF – le fournisseur d'un (ensemble) de services – peuvent être obtenus par leur utilisateur, la fonction SACF ou le processus d'application (AP) selon le cas.

L'interface avec les primitives de service est un élément théorique qui n'est ni essayable ni accessible. Il s'agit d'un outil descriptif. L'utilisation de primitives de service à une interface n'implique aucune implémentation particulière de celle-ci ni la nécessité qu'une implémentation soit conforme à cette interface particulière avec les primitives de service pour fournir le service indiqué. La conformité aux spécifications ISUP et TC est fondée sur le comportement externe d'un nœud, c'est-à-dire sur la génération de la structure correcte des messages (telle que spécifiée dans la référence [13]) et des opérations (telle que spécifiée dans la présente Recommandation), dans l'ordre approprié (tel que spécifié dans la référence [14] ainsi que dans la présente Recommandation).

La structure et des exemples de l'utilisation de cette interface sont décrits au 6.2.

La relation entre la capacité de réseau privé et les services du mécanisme de transport d'application fournis par l'interface NNI est décrite au 6.1 sous la forme d'un modèle de réseau. L'élément APM ASE apporte aux capacités ISUP les extensions nécessaires pour que les services offerts à l'utilisateur APM d'une association sémaphore nécessitant un support (l'application VPN en l'occurrence) soient semblables aux services offerts par le sous-système TCAP lorsque aucun support n'est requis.

Les spécifications relatives aux réseaux privés (référence [1]) renvoient aux primitives propres aux réseaux privés qui représentent les flux informationnels du système PSS1 entre commande d'appel et commande de protocole. Dans la présente Recommandation, le processus d'application décrit la relation entre ces primitives et entre celles-ci et les primitives appropriées du modèle de structuration ALS pour le transport des flux informationnels du système PSS1.

Le 11.1 contient des exemples du mécanisme de signalisation non associé à un support.

6 Modélisation

Les modèles décrits dans le présent paragraphe développent les concepts et les termes utilisés dans la présente spécification de l'utilisation, par l'application VPN, de la capacité du mécanisme de transport d'application (APM) pour la signalisation associée à un support et du sous-système gestionnaire de transactions (TC) pour la signalisation non associée à un support.

6.1 Modèle de réseau

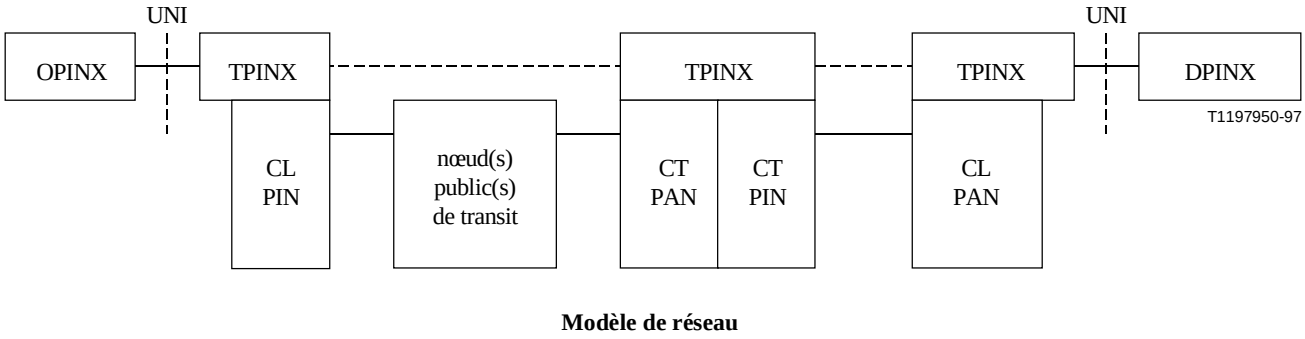


Figure 1/Q.765.1 – Exemple de topologie des nœuds PINX d'un réseau privé ainsi que de leurs relations avec le concept de nœuds PIN/PAN à l'interface avec le réseau public

Le présent sous-paragraphe décrit la relation entre le VPN et le réseau public pour la fourniture d'un service. La Figure 1 donne un exemple d'appel issu d'un nœud PINX d'origine vers un nœud PINX de destination via des nœuds PINX de transit. Ceux-ci sont, dans ce cas, implémentés dans l'infrastructure du réseau public, qui joue également le rôle de liaison entre les nœuds PINX de transit. Dans cet exemple, la liaison s'effectue via un autre nœud public de transit.

Le concept de nœud public initiateur (PIN, *public initiating node*) et de nœud public adressé (PAN, *public addressed node*) est introduit dans la référence [23] pour faciliter la description du mécanisme APM. Le nœud PIN représente le point du réseau où une application d'utilisateur APM (en l'occurrence le VPN) souhaite établir, pour la prise en charge d'une entité (PIN) de flux informationnels du système PSS1, des communications vers une application d'utilisateur APM homologue située à un point adressé (PAN) dans le réseau. Une application VPN pour la prise en charge de flux informationnels du système PSS1 peut donner lieu à l'établissement d'une association sémaphore et d'un circuit support, auquel cas elle utilisera les services de l'appel de base sur réseau public.

La capacité de nœud PINX demande les services du réseau public afin d'établir une association sémaphore avec le nœud PINX subséquent dans le réseau privé virtuel. L'application du nœud PINX initiateur fournit un numéro E.164 public normal qui est utilisé pour l'acheminement dans le réseau public et donc pour établir une association entre le nœud public initiateur (PIN) et le nœud public adressé (PAN). Celui-ci identifie l'application d'utilisateur APM particulière au moyen de la valeur d'identificateur de contexte qui est acheminée dans le paramètre de transport d'application (APP, *application transport parameter*). Dans ce cas, il s'agit de la valeur "PSS1 ASE (VPN)". Le nœud PAN identifie l'application PINX particulière associée à un réseau d'entreprise spécifique, identifié par un identificateur de réseau de télécommunication d'entreprise (par exemple un paramètre CNID).

La nature de la capacité de nœud PINX (c'est-à-dire nœud PINX d'origine, de destination, de transit ou de passerelle) est indépendante du mécanisme décrit ici et ne dépend que de la topologie du réseau privé virtuel.

Le mécanisme d'appel public de base sert à établir une association entre les nœuds PIN et PAN. Lors de son acheminement dans le réseau public, l'appel peut passer par des nœuds publics intermédiaires possédant ou ne possédant pas la capacité d'application privée. Cependant, étant donné que l'application privée n'est pas adressée par cette instance d'appel particulière, elle se comportera comme un nœud public intermédiaire normal.

La Figure 2 donne un exemple de séquence de messages sur le réseau public pour une communication nécessitant un support (ISUP) dans le scénario de la Figure 1. La Figure 3 montre la séquence d'opérations dans le réseau public (TC) pour une communication ne nécessitant pas de support.

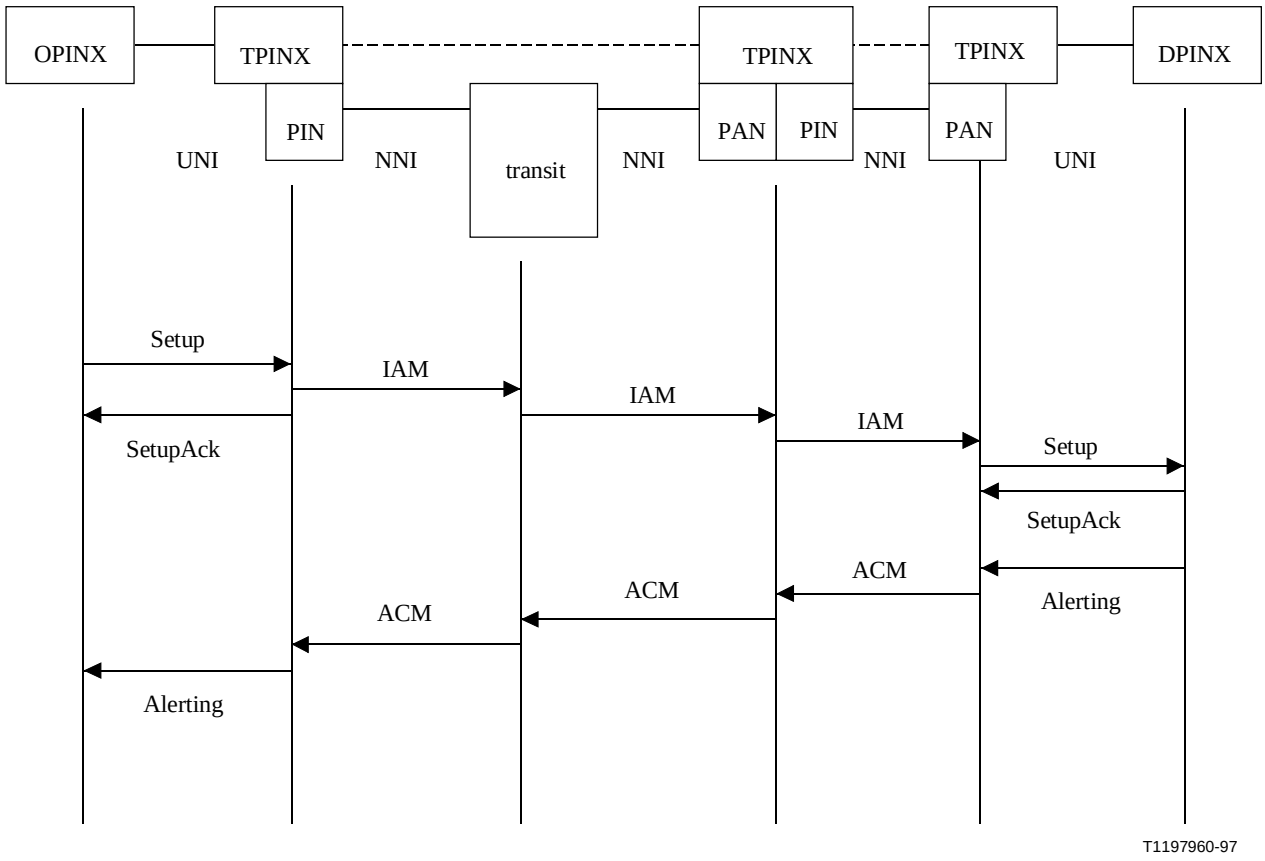


Figure 2/Q.765.1 – Exemple de séquence de messages pour appel avec support

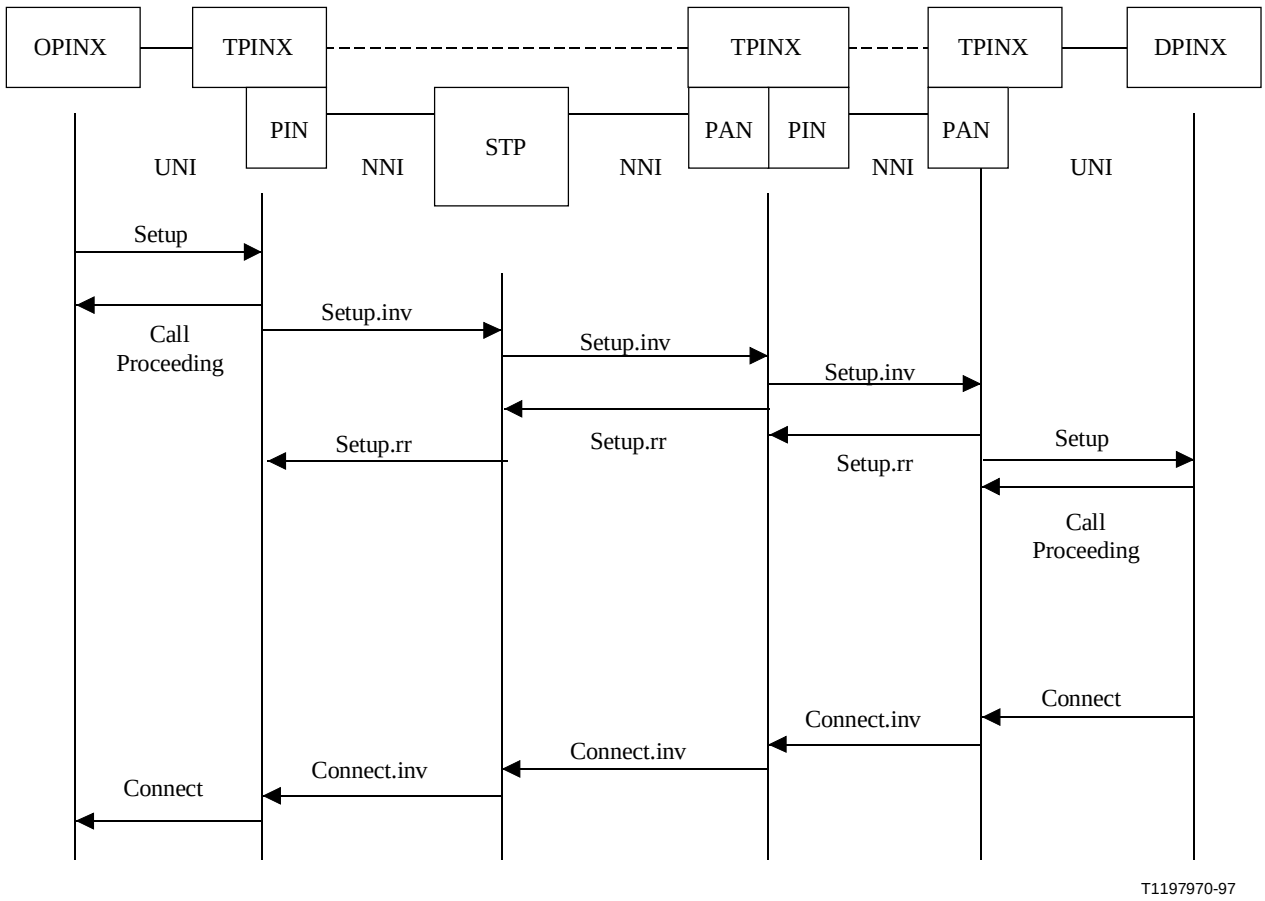


Figure 3/Q.765.1 – Exemple de séquence d'opérations pour appel sans support

6.2 Modèle de spécification

6.2.1 Introduction

Le modèle utilisé pour structurer la description des procédures d'application ISUP et TC-USER est fondé sur le modèle de structuration de la couche Application (ALS, *application layer structure*) de l'OSI (voir la référence [24]). Le présent sous-paragraphe présente ce modèle et donne une description générale de son fonctionnement. Il montre le modèle généralisé du "processus d'application de commutateur" permettant de prendre en charge des applications de flux informationnels PSS1 dans des réseaux privés virtuels (VPN) de part et d'autre de l'interface nodale avec le réseau (NNI) public. Il montre comment l'application utilise le mécanisme de transport d'application (APM, *application transport mechanism*) qui est décrit en détail dans la référence [23].

6.2.2 Modèle général

Le modèle généralisé qui représente le processus d'application VPN associé (ISUP) ou non associé (TC) au circuit support est illustré par la Figure 4. Celle-ci ne montre pas la situation à un point quelconque au cours des procédures ISUP mais donne l'image complète de l'architecture. L'application spécifique de ce modèle est étudiée ci-dessous. La Figure 4 montre les interfaces avec les primitives échangées entre les blocs fonctionnels, telles qu'elles sont utilisées dans le corps de la présente Recommandation pour les appels avec (ISUP) et sans (TC) support.

Les interfaces (a) à (k) sont définies comme suit:

(a) interface entre les fonctions nodales du processus d'application (AP) et la fonction SACF pour la prise en charge de flux informationnels PSS1 dans des applications VPN de part et d'autre de l'interface NNI: voir 7.2.2;

(b) interface avec les éléments PSS1 ASE, qui définit les formats et les codes dans le paramètre APP pour la prise en charge de flux informationnels PSS1 dans des applications VPN: voir 10.1;

(c) interface entre fonction SACF et éléments UCEH ASE, représentant le traitement des valeurs de non-identification de contexte et d'erreur associé au mécanisme de transport d'application: voir la référence [23];

(d) interface entre fonction SACF et éléments APM ASE, représentant des extensions de la capacité de réseau public (ISUP) pour la fourniture d'un mécanisme de transport assurant diverses applications (d'utilisateur APM) de part et d'autre de l'interface NNI: voir la référence [23] (cette interface est hors du domaine d'application de la présente Recommandation);

(e) interface avec les éléments ASE de signalisation d'appel de base ISUP: voir la référence [23] (cette interface est hors du domaine d'application de la présente Recommandation);

(f) interface entre fonction SACF et interface NI: voir la référence [23] (cette interface est hors du domaine d'application de la présente Recommandation);

(g) interface avec le sous-système MTP-3: voir la référence [23] (cette interface est hors du domaine d'application de la présente Recommandation);

(h) interface entre fonction TC SACF et AP: voir 7.3.2;

(i) interface entre fonction TC SACF et éléments COPSS1 ASE assurant la fonction de commande de protocole pour la signalisation en mode connexion sans support associé: voir 11.1;

(j) interface entre fonction TC SACF et éléments TC ASE assurant les services définis dans la référence [16]: voir 12.1;

(k) interface entre fonction TC SACF et sous-système SCCP, assurant les services définis dans la référence [7]: voir 13.1.

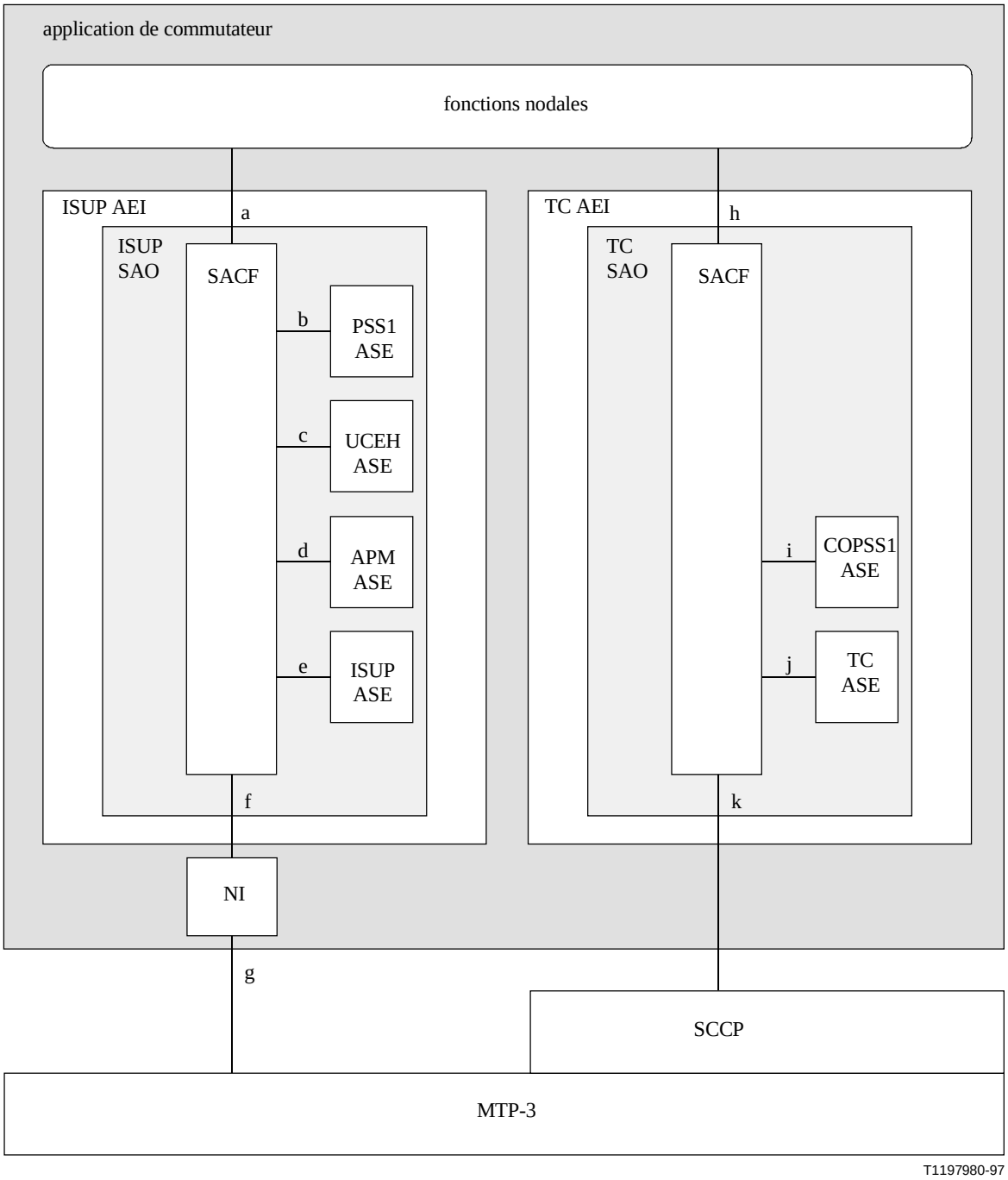


Figure 4/Q.765.1 – Modèle de spécification pour la signalisation ISUP et la signalisation en mode connexion

Concernant la Figure 4, toutes les fonctions ont également une interface avec une "application de gestion" qui n'est pas définie en tant qu'interface formelle avec des primitives.

Le terme "processus d'application de commutateur" sert à décrire toute la capacité applicative d'un commutateur. Le sous-système ISUP fait partie du processus d'application de commutateur. Les fonctions nodales ISUP représentées sur le modèle seront donc désignées, dans le corps de la présente Recommandation, par le terme "fonctions du processus d'application ISUP". De même, les fonctions nodales de gestionnaire de transactions sans support associé, représentées sur le modèle, seront désignées, dans le corps de la présente Recommandation, par le terme "fonctions de processus d'application TC".

L'entité ISUP/TC AEI fournit toutes les capacités de communication requises par les fonctions nodales ISUP/TC. Pour simplifier, une entité ISUP/TC AEI est définie comme ne contenant qu'un seul objet SAO. Cela évite la nécessité de spécifier une fonction de commande d'association multiple (MACF, *multiple association control function*). Toute la coordination des associations sémaphores ISUP est donc effectuée par les fonctions nodales ISUP. De même, la coordination des associations sémaphores TC est effectuées par les fonctions nodales TC.

La fonction SACF est chargée de coordonner correctement le flux de primitives entre ses interfaces.

L'élément ISUP ASE est défini par la référence [14]. Ses principales tâches sont d'assurer les procédures d'appel de base, le traitement des erreurs de protocole et le traitement des informations non reconnues. La nature monolithique de ces Recommandations implique que les deux fonctions de commande d'appel public de base et de commande de protocole soient définies de concert. La présente Recommandation ne vise pas à remanier la définition [14] pour lui donner la structuration ALS. Cette définition sera donc citée en référence, dans la présente Recommandation, sous l'appellation globale d'élément "ISUP ASE". Théoriquement, cet élément devrait être considéré comme représentant une subdivision logique entre la fonction de commande de protocole à l'intérieur de l'élément ISUP ASE et la fonction de commande d'appel qui lui est associée à l'intérieur du processus d'application. La modélisation et les interfaces correspondantes sont hors du domaine d'application de la présente Recommandation. (Voir la référence [23].)

L'élément APM ASE permet de transférer des informations entre des nœuds pour la signalisation devant passer par un circuit support. Il permet également de fournir des services génériques aux applications tout en conservant l'indépendance par rapport à elles. Cet élément est chargé des extensions de l'interface NNI (ISUP) pour la prise en charge d'un mécanisme permettant à diverses applications de transporter leurs flux d'information via l'interface NNI. Sa principale tâche est d'assurer la segmentation et le réassemblage des messages afin de donner à l'entité utilisatrice du mécanisme APM la capacité de transporter jusqu'à 2048 octets d'informations applicatives. L'élément APM ASE est en mesure de prendre en charge plusieurs utilisateurs APM, chacun étant traité indépendamment des autres et recevant le même niveau de service. Il se compose de deux ensembles fonctionnels distincts: l'un sert de nœud public adressé (PAN) et l'autre de nœud public initiateur (PIN, assurant l'association sémaphore vers le nœud PAN). Le concept PIN/PAN est expliqué au 6.1/Q.765 de la référence [23].

L'élément UCEH ASE constitue un mécanisme de compatibilité pour le cas où divers niveaux (de contexte) d'application existeraient à l'intérieur des nœuds du réseau. Cet élément traite également les cas d'erreur de réassemblage APM. Il est chargé des procédures associées à la réception d'un paramètre de transport d'application (APP) faisant référence à un identificateur de contexte non identifié. Il assure le traitement correspondant d'une notification signalant qu'un identificateur de contexte particulier n'est pas pris en charge dans un nœud distant (voir la référence [23]). Cet élément traite également les cas d'erreur de réassemblage APM.

L'élément PSS1 ASE est un utilisateur des services offerts par l'élément APM ASE. Il est chargé de préparer l'information sémaphore de réseau privé sous une forme transportable par le mécanisme de transport d'application (APM) du réseau public.

L'élément TC ASE permet de transférer des informations sémaphores internodales sans support. Il fournit également des services génériques aux applications, tout en restant indépendant de celles-là. L'élément TC ASE est défini dans les références [16] à [20].

L'élément COPSS1 ASE est un utilisateur des services offerts par l'élément TC ASE. Il se compose de deux ensembles fonctionnels distincts, associés au nœud public adressé (PAN) et au nœud public initiateur (PIN) lors d'une signalisation non associée au support en mode connexion (dialogue avec le gestionnaire TC).

Pour traiter toute fonction ISUP particulière, le processus d'application de commutateur crée une instance des fonctions nodales ISUP/TC requises. Le processus AP créera, en fonction des besoins, des instances de l'entité ISUP/TC AEI. La fonction d'interface avec le réseau (NI) existe pour distribuer des messages reçus du sous-système MTP-3 à l'instance appropriée de l'entité ISUP AEI. Dans un commutateur, il n'existe qu'une seule instance de l'interface avec le réseau. Les messages sont distribués aux instances TC AEI appropriées au moyen du numéro SSN et de l'identificateur de dialogue avec le gestionnaire TC. Le NI est décrit dans la référence [23].

L'interface avec le sous-système SCCP est décrite dans les références [7] à [12].

L'objet SAO contenu dans l'élément ISUP AE est de l'un des types suivants:

a) *nœud public initiateur (PIN)*

ce nœud contient:

- l'élément ISUP ASE sortant, l'élément APM ASE initiateur, l'élément UCEH ASE initiateur, l'élément PSS1 ASE sortant et la fonction ISUP SACF.

b) *nœud public adressé (PAN)*

ce nœud contient:

- l'élément ISUP ASE entrant, l'élément APM ASE adressé, l'élément UCEH ASE adressé, l'élément PSS1 ASE entrant et la fonction ISUP SACF.

L'objet SAO contenu dans l'entité d'application TC AE pour la signalisation en mode connexion non associée au support est de l'un des types suivants:

a) *nœud public initiateur (PIN)*

ce nœud contient:

- l'élément COPSS1 ASE sortant, l'élément TC ASE et la fonction TC SACF.

b) *nœud public adressé (PAN)*

ce nœud contient:

- l'élément COPSS1 ASE entrant, l'élément TC ASE et la fonction TC SACF.

6.2.3 Flux dynamique des primitives

6.2.3.1 Flux sémaphores associés au support

Les Figures 5 et 6 décrivent les flux dynamiques de primitives pour un appel VPN avec flux informationnels PSS1 pris en charge de part et d'autre de l'interface NNI (ISUP) dans le cas où un message de commande d'appel coïncide avec le flux informationnel de l'application. La Figure 5 montre l'émission et la Figure 6 la réception d'un message.

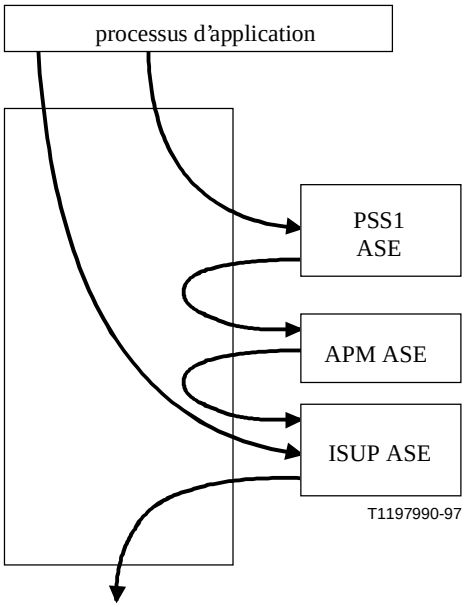


Figure 5/Q.765.1

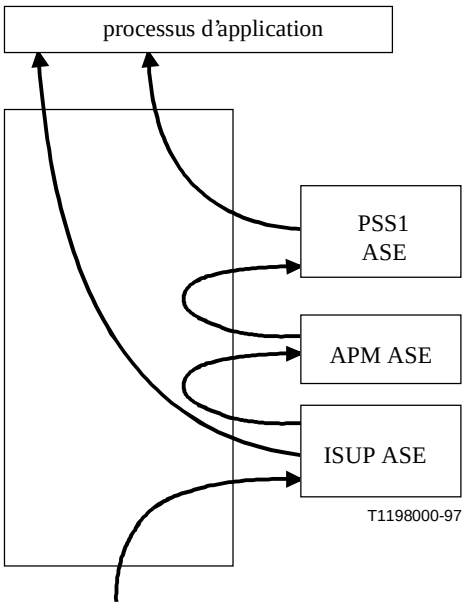


Figure 6/Q.765.1

Les Figures 7 et 8 décrivent les flux dynamiques de primitives pour la prise en charge par l'interface NNI des flux informationnels PSS1 d'un appel VPN dont les messages de commande d'appel ne sont pas envoyés en coïncidence avec ces flux. En d'autres termes, l'élément APM ASE lance une primitive vers l'élément ISUP ASE, qui à son tour envoie un message APM fournissant un mécanisme pour prendre en charge le flux informationnel.

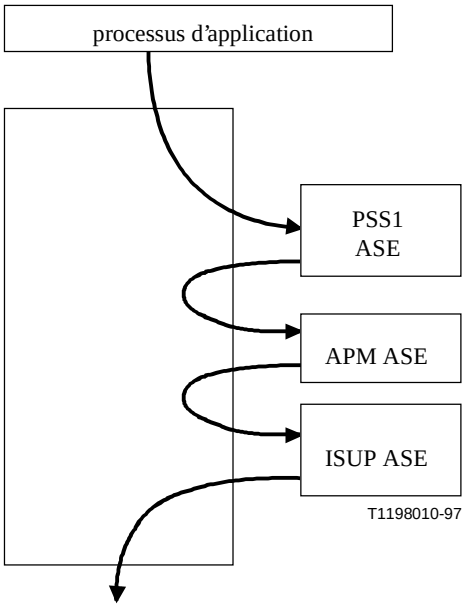


Figure 7/Q.765.1

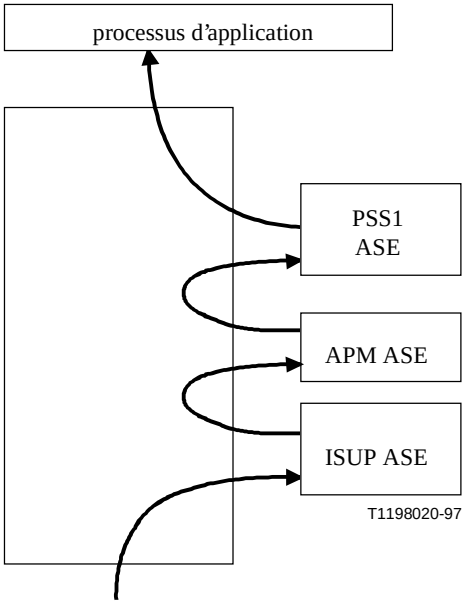


Figure 8/Q.765.1

6.2.3.2 Flux sémaphores non associés au support

Les Figures 9 et 10 décrivent les flux dynamiques de primitives pour une connexion de signalisation VPN sans association à un support de part et d'autre de l'interface NNI (TC).

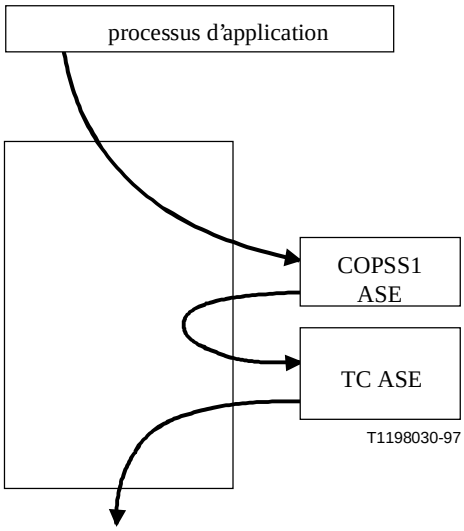


Figure 9/Q.765.1

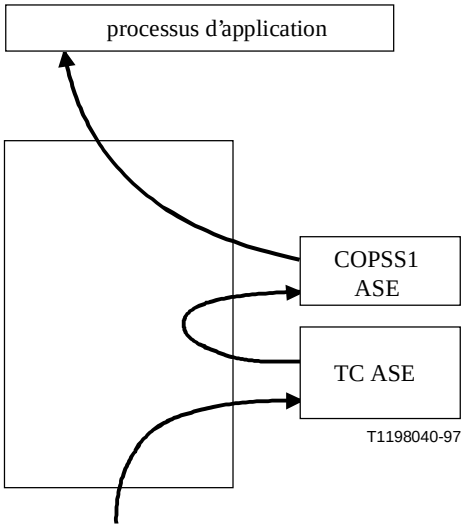


Figure 10/Q.765.1

6.2.4 Appel de base

Le réseau public peut être considéré comme un PINX virtuel de transit lors de l'établissement de communications VPN nécessitant la prise en charge de la continuité des informations PSS1 et répondant donc aux prescriptions fonctionnelles définies dans l'appel de base PSS1 pour un nœud PINX de transit.

Si une situation de repli se produit à l'intérieur du VPN (c'est-à-dire une perte de continuité des flux informationnels PSS1), le réseau public fournit la capacité de nœud PINX passerelle, jouant un rôle analogue à celui d'un nœud PINX passerelle interconnectant, à l'intérieur d'un réseau privé, un nœud PINX à un réseau public.

6.2.5 Fonction de nœud PINX de transit – Protocole fonctionnel générique

Deux cas doivent être distingués pour décrire les comportements du réseau public pour les appels VPN ou pour des connexions sémaphores VPN non associées au support afin d'assurer la continuité fonctionnelle des procédures PSS1-GF (c'est-à-dire du protocole fonctionnel générique (GFP) du système PSS1 pour la prise en charge de services complémentaires dans le réseau privé):

1) prise en charge complète de la capacité de protocole GFP: le VPN offre la capacité de nœud PINX de transit complète, telle que définie dans la fonction PSS1-GF (référence [3]), ce qui inclut l'analyse du champ d'extension NFE des éléments d'information de type "fonctionnalité" reçus;

2) la prise en charge partielle de la capacité de protocole GFP: le nœud du VPN remplit les mêmes fonctions que dans l'option 1, sauf pour le traitement de l'élément d'information "fonctionnalité" avec le profil de protocole mis à la valeur "extensions de réseautage". Le nœud du VPN transmettra en transparence, entre deux nœuds PINX directement connectés au VPN, les informations fonctionnelles PSS1-GF reçues dans un élément d'information "fonctionnalité", avec le profil de protocole mis à la valeur "extensions de réseautage".

L'utilisation de l'option 2 dans un réseau peut donner lieu au fonctionnement incorrect de certains services du réseau. Pour éviter ce problème, il est nécessaire de prévoir une topologie de réseautage telle qu'un nœud de ce type ne soit pas utilisé avec des services de ce type.

De part et d'autre de l'interface internationale, la capacité de l'option 1 peut être utilisée et prise en charge, tandis que l'option 2 peut faire l'objet d'un accord bilatéral entre opérateurs de réseau pour sa prise en charge de part et d'autre de l'interface internationale.

6.2.6 Fonction de nœud PINX passerelle

La capacité de nœud PINX passerelle (GPINX, *gateway PINX*) est invoquée lorsqu'on a déterminé que la continuité des flux informationnels PSS1 ne peut plus être assurée. Le nœud GPINX peut être invoqué à la suite d'une analyse démontrant que la destination ne prend pas en charge les flux informationnels PSS1 (voir la Note) ou à la suite d'une indication de non-prise en charge du transport des flux informationnels PSS1 par les canaux sémaphores du réseau intermédiaire, ou à la suite d'une indication de non-prise en charge du mécanisme APM ou de l'utilisateur APM dans le nœud PAN (voir 7.2.3.2.5).

NOTE – Cette capacité tient compte de la situation où le nœud PAN est l'entité DLE qui joue le rôle de nœud PINX de transit avec accès sortant prenant en charge les flux informationnels PSS1, mais où le nœud PAN libère l'appel avant d'envoyer la demande d'établissement d'appel à cet accès sortant.

Si l'on détermine que la continuité des flux informationnels PSS1 ne peut pas être conservée, deux options se présentent:

1) laisser l'appel progresser (choisir de remplir la fonction de passerelle ou demander qu'elle soit remplie ailleurs);

2) libérer l'appel.

Si l'appel est autorisé à progresser, il est nécessaire que les informations d'appel de base dans le réseau public pour acheminer l'appel VPN soient suffisantes pour permettre à cet appel de progresser et d'aboutir normalement. L'utilisation de ces options relève d'un choix des opérateurs de réseau sur la base du niveau de service offert au propriétaire du réseau privé.

La prise en charge du protocole fonctionnel générique (GFP, *generic functional protocol*) dans le cadre de la capacité de nœud PINX passerelle est facultative selon l'ISO/CEI 11582 [3]. Le choix est donc laissé à l'opérateur de réseau de prendre en charge les procédures de traitement du protocole fonctionnel générique. Il faut relever que certains services peuvent se comporter d'une façon tout sauf souhaitable si le protocole GFP n'est pas pris en charge.

Pour réduire l'effet de charge sémaphore dans le réseau due à la prise en compte des flux informationnels PSS1 dans le VPN, l'opérateur de réseau a la possibilité d'activer le mécanisme de déplacement de la capacité de nœud GPINX pour la rapprocher autant que possible de l'extrémité d'origine du conduit de communication. Deux options existent:

a) fonction GPINX assurée au point de "rupture":

   exécution de la fonction de nœud PINX passerelle au point du réseau où l'on détermine que cette passerelle est requise;

b) fonction GPINX assurée par coopération internodale (déplacement de la capacité de passerelle vers un point amont dans le conduit de communication):

   exécution de la fonction de nœud PINX passerelle lorsque le nœud qui détermine que cette fonction est requise exécute pour le message IAM la fonction de passerelle pour "appel de base" (et exécute la fonction de passerelle fonctionnelle générique s'il peut la gérer). Si ce nœud a été informé du fait qu'un nœud antérieur possède la capacité de fournir la fonction de passerelle (indication de capacité de transformation en passerelle reçue dans le message IAM envoyé par un nœud amont sur le conduit de communication), ce nœud envoie en amont la demande correspondante. Lorsque le nœud antérieur possédant la capacité de transformation en passerelle d'un nœud PINX reçoit cette demande, il exécute la fonction de passerelle (d'appel de base et, s'il le peut, fonctionnelle générique) à partir de ce moment pour cette communication.

7 Fonctions du processus d'application

7.1 Généralités

La modélisation du processus d'application (AP) est hors du domaine d'application de la présente Recommandation. Afin d'évaluer le rôle de ce processus par rapport aux objectifs de la présente Recommandation, l'on peut cependant le considérer comme étant composé de trois types différents de capacité, applicables à la prise en charge des réseaux privés de part et d'autre de l'interface nodale avec le réseau public. Il s'agit du mécanisme de transport d'application sur réseau public (défini dans la référence [23]); de l'appel de base ISUP [14]; et des applications de réseau privé virtuel (VPN) pour la prise en charge du système PSS1, tel que défini dans la présente Recommandation.

L'aspect de la capacité de processus d'application qui est introduit par la présente Recommandation est la coordination requise entre réseaux publics et privés virtuels pour la prise en charge et le transport approprié des flux informationnels PSS1:

- soit au moyen de la combinaison du mécanisme d'appel public de base ISUP et du mécanisme de transport d'application;
- soit au moyen des mécanismes de gestion des transactions.

La capacité de réseau privée offerte par le VPN est décrite dans les 6.2.4, 6.2.5 et 6.2.6. Pour montrer la relation entre le processus d'application VPN et la logique de commande d'appel PSS1, la présente Recommandation définit le mappage entre primitives de commande d'appel/commande de protocole

[2] et primitives SACF à l'interface (a). Elle décrit également les procédures supplémentaires propres au VPN. La description des processus d'application sur réseau public ou sur nœud PINX est hors du domaine d'application de la présente Recommandation.

La définition de l'interface avec les primitives entre processus d'application et fonction SACF pour le mécanisme APM sur réseau public est hors du domaine d'application de la présente Recommandation.

7.2 Fonctions du processus d'application VPN – Connexion avec communication (associée au support)

7.2.1 Introduction

La fonction de l'aspect du processus d'application (AP) qui concerne la prise en charge des applications VPN par l'interface NNI avec le réseau public consiste à assurer la coordination entre les fonctions de processus d'application sur réseau privé (système PSS1) et de processus d'application sur réseau public. Lorsque l'application privée nécessite l'établissement d'une association sémaphore avec support, le processus d'application convertit les informations d'adressage privé pour leur donner la forme que le processus d'application public peut utiliser afin d'acheminer l'appel depuis le nœud public initiateur (PIN) jusqu'au commutateur approprié du réseau public (nœud public adressé, PAN) qui contient la fonction adjacente de nœud PINX. Le concept de nœuds PIN/PAN est décrit dans la référence [23]. L'utilisation de ce concept pour un réseau privé spécifique est décrite au 6.1. On peut trouver des détails sur les informations requises pour l'acheminement d'un appel public de base dans la référence [14]. La conversion des informations privées en une forme appropriée à l'acheminement dans le réseau public est hors du domaine d'application de la présente Recommandation. La façon dont les informations appropriées d'acheminement public sont produites relève du réseau (il peut par exemple s'agir du résultat d'une analyse locale ou de l'emploi de mécanismes du réseau intelligent).

La présente Recommandation ne vise pas à redéfinir la capacité de nœud PINX dans le système PSS1. La commande d'appel définie dans la référence [1] est donc applicable. La présente Recommandation vise à décrire la façon dont sont assurés dans un VPN, de concert avec l'appel de base ISUP et le mécanisme APM, les services attendus par le système PSS1 à l'interface (définie dans la référence [2]) entre commande d'appel (CC, *call control*) et commande de protocole (PC, *protocol control*), afin de réaliser la continuité des flux informationnels PSS1 de part et d'autre de l'interface NNI avec le réseau public.

Le maintien de l'alignement des états de l'appel public de base et de la commande d'appel du système PSS1 relève du processu d'application VPN.

L'interface entre primitives PSS1 de commande d'appel et de commande de protocole (voir le modèle ISO/CEI, dans la référence [2]) et l'interface entre les primitives de commande de transport générique fonctionnel (GFT) et les primitives de commande de protocole (voir le modèle ISO/CEI dans la référence [3]) ne sont pas visibles en tant qu'interfaces dans la structure ALS. La présente Recommandation vise, non pas à modéliser le processus d'application mais à illustrer la relation entre son contenu et la capacité de nœud PINX qui est définie par l'ISO, comme représenté sur la Figure 11. L'applicabilité des fonctions de commande d'appel PSS1 et de protocole fonctionnel générique PSS1, représentées sur la Figure 11, dépend de la fourniture de la capacité PINX par un nœud.

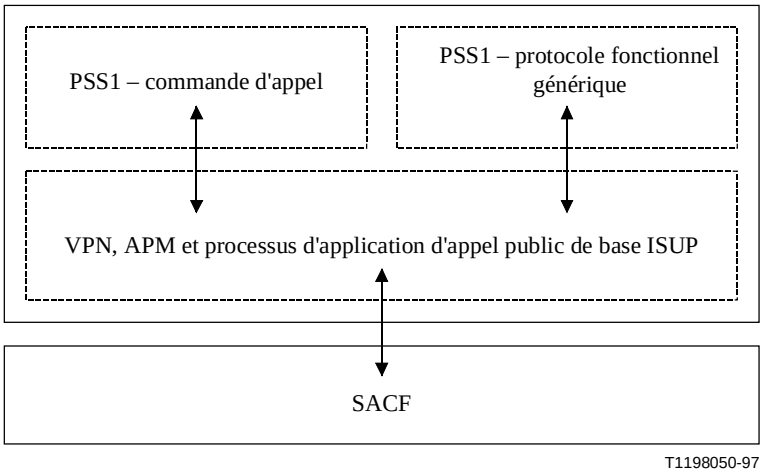


Figure 11/Q.765.1 – Relation entre interfaces avec les primitives PSS1 et le modèle ALS

De façon à maintenir la continuité des flux informationnels PSS1 dans un réseau privé virtuel, il est nécessaire d'introduire des procédures additionnelles permettant aux VPN de coexister dans le réseau public et de gérer les scénarios propres à leur prise en charge dans ce réseau. Ces procédures comportent la possibilité d'utiliser un identificateur de réseau de télécommunication d'entreprise (CNID, *corporate telecommunications network identifier*) afin d'identifier de façon unique un réseau d'entreprise; la possibilité de transférer des identités VPN et le réglage approprié des indicateurs d'instruction de transport d'application (ATII, *application transport instruction indicators*) afin de tenir compte des cas d'erreur.

Lors de l'établissement de l'appel, la capacité de nœud PINX située dans le nœud PAN détermine si des chiffres privés additionnels doivent être reçus (numérotation avec chevauchement de chiffres privés). Dans ce cas, il est nécessaire que le nœud PAN renvoie au nœud PIN une indication d'acquittement d'établissement afin de confirmer l'association sémaphore dans le réseau et afin que le nœud PIN puisse envoyer au nœud PAN des chiffres additionnels de manière fiable.

Pour que les appels VPN demandant la prise en charge des flux informationnels PSS1 puissent fonctionner correctement, il est nécessaire que les nœuds publics intermédiaires entre PIN et PAN possèdent la capacité de signalisation nécessaire pour transporter le paramètre APP. Si le canal ou les canaux subséquents ne prennent pas en charge le mécanisme APM et qu'ainsi les informations VPN transportées soient perdues, ou si le nœud adressé ne possède pas la capacité APM ou PINX, le nœud doit invoquer la capacité de nœud PINX passerelle qui est décrite au 6.2.6. Cette capacité sémaphore peut ne pas être mise à contribution si l'appel est acheminé par des nœuds tels qu'un nœud ISUP selon Q.767 [15], un nœud passerelle du réseau public ou un nœud à protocole non ISUP. Pour traiter le cas où les nœuds intermédiaires et leurs capacités sémaphores associées ne peuvent pas prendre en charge le transport de flux informationnels PSS1 au moyen du mécanisme de transport d'application, ou pour traiter le cas où l'appel s'adresse à un nœud sans capacité APM ou PINX-PSS1 et est autorisé à progresser (option réseau), il est nécessaire de disposer d'un mécanisme confirmant que le VPN peut prendre en charge les flux informationnels PSS1 [indication de "capacité de transparence aux éléments VPN" (VTI)]. Il est également nécessaire d'informer le nœud PINX précédent qu'il doit invoquer la capacité de PINX passerelle. Le mécanisme d'invocation de la fonction de passerelle doit être implicite dans l'invocation de la capacité GPINX dans les cas suivants:

- non-réception d'une confirmation de prise en charge de la continuité des flux informationnels PSS1 [indication de "capacité de transparence aux éléments VPN" (VTI)];
- réception d'une notification contenant la valeur "non-identification du contexte";

- réception d'un message d'incohérence dont le champ de diagnostic indique que le paramètre APP a été ignoré.

Dans un tel cas, le nœud doit déterminer s'il y a lieu de libérer immédiatement l'appel ou de le laisser progresser. (Il s'agit d'une option de l'opérateur du réseau, fondée sur le niveau de service offert au propriétaire du réseau privé.) Si l'appel est autorisé à progresser, il faut que les informations d'appel public de base soient suffisantes pour qu'il puisse aboutir normalement.

Lorsque le "nœud déterminant que la capacité de nœud PINX passerelle doit être invoquée" a déterminé cette nécessité, ce nœud peut (option réseau) demander à un nœud PINX situé plus près de l'extrémité d'origine de l'appel (appelé "nœud possédant la capacité de transformation en PINX passerelle") de remplir la fonction de passerelle pour réduire la charge sémaphore imposée au réseau public par le réseau privé. Un mécanisme a été introduit pour permettre cette transformation, en nœud PINX passerelle sortant, d'un nœud PINX d'origine ou de transit situé plus en amont dans le conduit de communication. Ce mécanisme est fondé d'une part sur l'envoi en aval, par le nœud, d'une indication du fait qu'il possède la capacité d'effectuer la transformation et d'autre part sur l'envoi en amont, par un nœud subséquent, d'une demande de transformation en nœud PINX passerelle après détermination que la fonction de passerelle est requise.

7.2.2 Interface avec les primitives (AP-ISUP SACF)

L'interface [(a) sur la Figure 4] avec les primitives entre le processus AP et la fonction ISUP SACF repose sur les primitives nécessaires pour prendre en charge la capacité d'appel de base dans le réseau public et la capacité de réseau privé virtuel (VPN). Les primitives associées à la capacité de réseau public sont hors du domaine d'application de la présente Recommandation bien qu'il y soit fait référence au moyen de citations fonctionnelles dans le texte. La Recommandation concernant l'appel public de base n'est pas décrite en termes de concepts structurels ALS: il est donc nécessaire que les citations fonctionnelles se rapportent à la capacité d'appel public de base plutôt qu'à des primitives spécifiques. La présente Recommandation décrit les primitives associées à la capacité VPN. Voir le Tableau 2.

Tableau 2/Q.765.1– Primitives entre AP et ISUP SACF (prise en charge d'un réseau privé virtuel)

Nom de la primitive	Types	Sens (Note)
PSS1_Data	Indication/Demande	➔ / ←
PSS1_Error	Indication	➔
Remote_Status	Indication	➔
NOTE – Flux de primitives de SACF à AP: ➔ Flux de primitives d'AP à SACF: ←		

7.2.3 Procédures

7.2.3.1 Flux informationnels PSS1

Les descriptions du service de réseau privé sont définies par l'ISO dans la série de normes internationales décrivant le réseau privé à intégration de services. Ceux-ci sont construits conformément à la norme relative aux services supports à 64 kbit/s en mode circuit (références [1] et [2]) et conformément au protocole fonctionnel générique pour la prise en charge de la norme sur les services complémentaires [3]. La prise en charge des services de réseau privé dans un réseau privé virtuel est obtenue par le transport des flux informationnels nécessaires dans les canaux sémaphores

du réseau public entre entités prenant en charge les descriptions de service de réseau privé. Les Tableaux 3, 4 et 5 décrivent la façon dont les flux informationnels PSS1 sont répartis entre les primitives à l'interface AP/SACF.

Tableau 3/Q.765.1 – Mappages entre primitives PSS1 définies dans la référence [2] et primitives AP/ISUP SACF

Primitives en direction/ provenance de l'Interface CC (référence [2])		Flux	Messages ISUP	Primitives en direction/ provenance de l'Interface AP/SACF (PSS1 ASE)
PC_SETUP	dem.	→	IAM	+PSS1_DATA Req
	ind.	←	IAM	+PSS1_DATA Ind
	rép.	→	ANM/CON	+PSS1_DATA Req
	conf.	←	ANM/CON	+PSS1_DATA Ind
PC_MORE_ INFORMATION	dem.	→	APM/ACM	+PSS1_DATA Req
	ind.	←	APM/ACM/CPG	+PSS1_DATA Ind
PC_INFORMATION	dem.	→	APM	+PSS1_DATA Req
	ind.	←	APM	+PSS1_DATA Ind
PC_PROCEED	dem.	→	ACM/CPG	+PSS1_DATA Req
	ind.	←	ACM/CPG	+PSS1_DATA Ind
PC_ALERTING	dem.	→	ACM/CPG	+PSS1_DATA Req
	ind.	←	ACM/CPG	+PSS1_DATA Ind
PC_PROGRESS	dem.	→	ACM/CPG	+PSS1_DATA Req
	ind.	←	ACM/CPG	+PSS1_DATA Ind
PC_REJECT	dem.	→	PRI/REL	+PSS1_DATA Req (PRI seulement)
	ind.	←	PRI/REL	+PSS1_DATA Ind (PRI seulement)
PC_DISCONNECT	dem.	→	PRI/REL	+PSS1_DATA Req (PRI seulement)
	ind.	←	PRI/REL	+PSS1_DATA Ind (PRI seulement)
PC_RELEASE	dem.	→	PRI/REL	+PSS1_DATA Req (PRI seulement)
	ind.	←	PRI/REL	+PSS1_DATA Ind (PRI seulement)
DL_RESET	ind.		s/o	

Tableau 4/Q.765.1 – Mappages entre primitives PSS1 définies dans la référence [5] et primitives AP/ISUP SACF

Primitives en direction/ provenance de l'Interface CC (référence [5])		Flux	Messages ISUP	Primitives en direction/ provenance de l'Interface AP/SACF (PSS1 ASE)
PC_TRANSIT_COUNTER	dem.	→	IAM	+PSS1_DATA Req
	ind.	←	IAM	+PSS1_DATA Ind

Tableau 5/Q.765.1 – Mappages entre primitives PSS1 définies dans la référence [3] et primitives AP/ISUP SACF

Primitives en direction/ provenance de l'Interface CC (référence [3])		Flux	Messages ISUP	Primitives en direction/ provenance de l'Interface AP/SACF (PSS1 ASE)
PC_DATA	dem.	→	IAM/ACM/ANM/CON/CPG/PRI/APM	+PSS1_DATA Req
	ind.	←	IAM/ACM/ANM/CON/CPG/PRI/APM	+PSS1_DATA Ind
PC_NOTIFY	dem.	→	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 Indications et procédures à l'interface NNI

Pour prendre en charge les flux informationnels PSS1 dans le réseau public et permettre au réseau privé virtuel de coexister avec l'environnement du réseau public, il est nécessaire d'introduire des procédures et flux informationnels supplémentaires.

7.2.3.2.1 Traitement des informations d'adressage

Procédures au nœud PIN

Le numéro de l'appelé qui a été inséré dans la primitive de demande PSS1_Data lors de l'établissement de l'appel est également (option nationale) transféré dans le message IAM contenant le paramètre numéro ISUP générique avec le champ indicateur de la partie qualificative du numéro mis à la valeur "numéro additionnel de l'appelé".

Le numéro de l'appelant qui a été inséré dans la primitive de demande PSS1_Data lors de l'établissement de l'appel est également (option nationale) transféré dans le message IAM contenant le paramètre numéro ISUP générique avec le champ indicateur de la partie qualificative du numéro mis à la valeur "numéro additionnel de l'appelant", sans tenir compte des services complémentaires CLIR et CLIP du réseau public.

Le numéro connecté qui a été reçu dans la primitive d'indication PSS1_Data en même temps que la primitive correspondant au message CON ou ANM, ainsi que la sous-adresse connectée qui a été reçue conformément aux procédures d'appel public de base, sont transférés vers le système de signalisation du réseau d'accès sans tenir compte des services complémentaires COLP et COLR du réseau public.

Procédures du nœud PAN

Le numéro de l'appelant qui a été reçu dans la primitive d'indication PSS1_Data en même temps que le message IAM, ainsi que la sous-adresse de l'appelant qui a été reçue conformément aux procédures d'appel public de base, sont transférés vers le système de signalisation du réseau d'accès sans tenir compte des services complémentaires CLIP et CLIR éventuels du réseau public.

Le numéro connecté envoyé dans la primitive de demande PSS1_Data en même temps que la primitive correspondant au message CON ou ANM est transféré sans tenir compte des services complémentaires COLP et COLR du réseau public, dans la primitive correspondant au message CON ou ANM.

La sous-adresse connectée est transférée conformément aux procédures de l'appel public de base sans tenir compte des services complémentaires COLP et COLR du réseau public.

7.2.3.2.2 Identificateur de réseau de télécommunication d'entreprise

L'identificateur de réseau de télécommunication d'entreprise (CNID) est fourni à l'accès entrant de l'interface usager-réseau (UNI, *user-network interface*) ou possède une valeur implicite liée à l'accès entrant. L'identificateur CNID n'est requis que pour l'établissement d'appel [message IAM (ISUP)]. Il est obligatoire de part et d'autre de l'interface internationale et possède une portée mondiale. L'opérateur de réseau dispose de l'option d'employer un autre mécanisme pour identifier un réseau de télécommunication d'entreprise dans son propre domaine. Dès réception d'un identificateur CNID non reconnu par le nœud PAN, l'appel doit être libéré avec la cause n° 63 (service ou option non disponible – non spécifiée) et la fonction de gestion doit en recevoir notification.

7.2.3.2.3 Indicateurs d'instruction de transport d'application

Il est nécessaire que les indicateurs d'instruction de transport d'application (ATII) soient envoyés en même temps que d'éventuelles informations propres au réseau privé afin de traiter des cas d'erreur tels qu'une non-identification de contexte au nœud PAN ou des erreurs de réassemblage. Ces indicateurs doivent être réglés conformément aux besoins particuliers de l'application. En d'autres termes, si la capacité demandée est essentielle pour l'appel, les indicateurs ATII doivent être réglés de façon à libérer l'appel en cas d'erreur. En variante, si des actions doivent être effectuées pour traiter sans heurt un cas d'échec de communication mais avec progression de l'appel, il y a lieu de demander une notification. S'il n'y a aucun besoin réel d'indiquer un échec de communication avec le nœud PAN, aucune action n'a besoin d'être demandée dans les indicateurs ATII.

7.2.3.2.4 Acquittement par l'application homologue (numérotation avec chevauchement)

Procédures au nœud PAN

Dès réception de la primitive de demande PC_More_Information, le processus d'application envoie une primitive de demande PSS1_Data indiquant "acquittement d'établissement", déclenchant ainsi l'envoi d'un message APM vers le nœud PIN.

Procédures au nœud PIN

Dès réception de la primitive d'indication PSS1_Data indiquant "acquittement d'établissement", le processus d'application envoie une primitive d'indication PC_More_Information. Le nœud PIN doit envoyer le reste des chiffres privés du numéro de l'appelé (s'ils existent) en les insérant dans le paramètre numéro de l'appelé d'une ou de plusieurs primitives de demande PSS1_Data, donnant lieu à un ou à plusieurs messages APM. Le paramètre fin de numérotation peut lui aussi être envoyé selon les procédures de chevauchement des commandes d'appel PSS1.

7.2.3.2.5 Non-prise en charge par le nœud subséquent du mécanisme APM ou du réseau VPN

Procédures au nœud PAN

Lorsqu'un appel est en cours d'établissement avec la capacité PSS1 de transparence aux éléments de réseau, cet appel demande implicitement cette capacité par la présence du paramètre APP dans le message IAM, avec le champ d'identificateur de contexte d'application codé à la valeur "PSS1 ASE (VPN)". Si le nœud PAN détermine que l'appel VPN prend en charge la continuité des flux informationnels PSS1, ce nœud PAN doit insérer, dans le premier message vers l'amont contenant un paramètre APP, l'indication "appel avec capacité de transparence aux éléments VPN (VTI)".

Procédures au nœud PIN

Dès réception dans le nœud PIN de l'indication "appel avec capacité de transparence aux éléments VPN (VTI)" contenue dans un message ACM, CPG, CON, ANM, PRI ou APM, ce nœud PIN doit appliquer les procédures définies pour les appels VPN avec continuité des flux informationnels

PSS1. Après l'envoi d'un message IAM, le nœud PIN ne doit pas envoyer de paramètres APP (contenant des éléments d'information ou des notifications de type "extensions de réseautage" dans le champ "Fonctionnalité") avant la réception de l'indication "appel avec capacité de transparence aux éléments VPN" (VTI). De telles informations peuvent être ignorées.

Si l'option de laisser les appels progresser sans association applicative est prise en charge, la capacité de nœud PINX passerelle doit être invoquée pour les cas suivants. Le nœud PINX passerelle est décrit dans le 6.2.6.

- dès réception par le sous-système ISUP d'un message d'incohérence contenant un paramètre de cause de type "service inexistant ou non implémenté, service ignoré" (99) avec des diagnostics indiquant ce paramètre APP; (dans ce cas le mécanisme APM n'est pas pris en charge dans un nœud subséquent);
- dès réception d'une notification selon laquelle l'utilisateur APM homologue n'était pas présent dans le nœud PAN [paramètre APP avec champ d'identificateur de contexte d'application codé à la valeur "Elément ASE de traitement de non-identification de contexte et d'erreur (UCEH ASE)" et avec champ d'information de notification de transport d'application codé aux valeurs "Elément PSS1 ASE (VPN)" (dans le sous-champ d'identificateur de contexte d'utilisateur APM) et "Non-identification de contexte" (dans le sous-champ de cause), cette notification ayant été reçue dans un message ACM, CON, ANM, CPG, APM ou PRI];
- dès réception de la primitive correspondant au message CON sans aucun paramètre APP codé (dans le champ d'informations ACI) à la valeur "Elément PSS1 ASE (VPN)" et non-réception d'un message antérieur avec l'indication "appel avec capacité de transparence aux éléments VPN";
- dès réception de la primitive correspondant au message ANM sans aucun paramètre APP codé (dans le champ d'informations ACI) à la valeur "Elément PSS1 ASE (VPN)" et non-réception d'un message antérieur avec l'indication "appel avec capacité de transparence aux éléments VPN";
- dès réception de la primitive correspondant au message REL si l'indication "appel avec capacité de transparence aux éléments VPN" n'a pas été reçue dans un message antérieur;
- dès réception de la primitive correspondant au message ACM, indiquant "sans abonné" et non-réception d'un message antérieur contenant l'indication "appel avec capacité de transparence aux éléments VPN";
- dès réception de la primitive correspondant au message CPG, indiquant "alerte" sans aucun paramètre APP codé (dans le champ d'informations ACI à la valeur "Elément PSS1 ASE (VPN)" et non-réception d'un message antérieur contenant l'indication "appel avec capacité de transparence aux éléments VPN".

Si l'option de laisser les appels progresser sans association applicative n'est pas prise en charge, la réception des indications ci-dessus (selon lesquelles l'appel ne prend pas en charge la continuité des flux informationnels PSS1), l'appel doit être libéré avec la cause 63 (service ou option non disponible – non spécifiée) et les fonctions de gestion doivent en recevoir notification.

7.2.3.2.6 Mécanisme de demande de transformation en nœud PINX passerelle (option réseau)

Il y a lieu de noter que l'emploi de ce mécanisme a pour effet de supprimer les nœuds PINX de transit (intermédiaires) entre le "nœud possédant la capacité de transformation en PINX passerelle" et le "nœud déterminant que la capacité de nœud PINX passerelle doit être invoquée". La topologie du réseau doit donc être prise en compte lors de l'emploi de ce mécanisme.

La réception de l'indication "demande de transformation en nœud PINX passerelle" a priorité sur les procédures décrites au 7.2.3.2.5 qui peuvent être invoquées dès réception de l'indication "capacité de transparence aux éléments VPN (VTI)".

Nœud possédant la capacité de transformation en PINX passerelle

Un nœud remplissant les fonctions PINX (d'origine ou de transit) et possédant la capacité de se transformer en nœud PINX passerelle ("nœud possédant la capacité de transformation en PINX passerelle") doit insérer l'indication "nœud PINX avec capacité de transformation en passerelle" dans le message d'établissement initial envoyé vers l'aval.

Dès réception d'un indication de "demande de transformation en nœud PINX passerelle" contenue dans un message ACM, CPG, CON, ANM, PRI ou APM, un nœud doit vérifier les enregistrements en mémoire pour déterminer si un nœud antérieur possède la capacité de se transformer en nœud PINX passerelle. Si ce n'est pas le cas, le nœud doit transformer ses fonctions PINX pour se comporter comme un nœud PINX passerelle sortant pour toutes les informations propres aux réseaux privés qu'il recevra par la suite. Les procédures décrites au 7.2.3.2.5 pour le nœud PAN doivent s'appliquer lorsque la fonction de nœud PINX passerelle sera invoquée, en particulier l'envoi en amont de l'indication "appel avec capacité de transparence aux éléments VPN (VTI)", si cette indication n'a pas déjà été envoyée.

Nœud intermédiaire

Tout nœud remplissant les fonctions PINX, postérieur au "nœud possédant la capacité de transformation en nœud PINX passerelle", doit enregistrer dans sa mémoire qu'un nœud antérieur possède cette capacité. Il doit également envoyer la même indication en aval.

Dès réception d'une indication "demande de transformation en nœud PINX passerelle", un nœud doit vérifier l'enregistrement en mémoire pour déterminer si un nœud antérieur possède la capacité de se transformer en nœud PINX passerelle. Si tel est le cas, la demande est transmise sans changement.

Le nœud doit continuer à jouer le rôle de nœud PINX de transit pour toutes informations PSS1 reçues par la suite. Ces informations peuvent continuer à être reçues jusqu'à ce que la demande de transformation en nœud PINX passerelle ait été traitée par le "nœud possédant la capacité de transformation en nœud PINX passerelle".

Nœud déterminant que la capacité de nœud PINX passerelle doit être invoquée

Un nœud remplissant les fonctions PINX, déterminant qu'une capacité de nœud PINX passerelle doit être invoquée ("nœud déterminant que la capacité de nœud PINX passerelle doit être invoquée") doit appliquer les actions appropriées aux informations propres au réseau privé qui ont été reçues conformément à la définition donnée par l'ISO (voir 6.2.6).

Il doit ensuite, sur option réseau, vérifier l'enregistrement en mémoire pour déterminer si un nœud antérieur possède la capacité de se transformer en nœud PINX passerelle. Si cette capacité est disponible, le nœud doit envoyer en amont une "demande de transformation en nœud PINX passerelle" ainsi que l'indication "capacité de transparence aux éléments de service VPN (VTI)" mise à la valeur "pas d'indication".

Le nœud continuera à fonctionner comme un nœud PINX passerelle pour toute information PSS1 ultérieure reçue. Il sera possible de continuer à recevoir de telles informations jusqu'à ce que la demande de transformation en nœud PINX passerelle ait été traitée par le nœud possédant la capacité de transformation en nœud PINX passerelle".

7.2.3.4 Nœud relais

La capacité de nœud relais permet d'identifier les appels VPN et de les relayer vers des fonctions de nœud PINX désignées et simulées par l'équipement du réseau public, ou vers un nœud PINX physique désigné. Ce relais peut s'effectuer au moyen d'une autre capacité de nœud relais, comprenant le traitement en transparence des informations relatives aux réseaux privés.

Un nœud relais permet à un réseau de fournir la capacité de nœud PINX à distance d'un accès par interface UNI. Un nœud relais ne possède pas la capacité de nœud PINX mais offre un lien transparent entre un accès et le nœud qui contient la capacité PINX dans le réseau.

Lorsque le nœud relais a besoin d'établir une association sémaphore avec un support, le processus d'application produit des informations de routage dans le réseau public, sous une forme que le processus d'application public peut utiliser pour acheminer l'appel entre le nœud public initiateur (PIN) et le commutateur approprié dans le réseau public (nœud public adressé, PAN), qui contient la capacité PINX. On peut trouver dans la référence [14] des détails relatifs aux informations requises pour l'acheminement d'un appel public de base. Ces informations sont implicitement liées à l'identificateur CNID associé à l'accès.

Le nœud relais prend en charge les flux informationnels PSS1 d'interfonctionnement entre les protocoles de l'interface usager-réseau (UNI) et de l'interface nodale avec le réseau (NNI). Les informations propres aux réseaux privés sont transmises en transparence et réparties entre les primitives passant par l'interface AP/ISUPS ACF de la même façon que les informations reçues de la logique de commande d'appel privé, ce qui permet d'assurer la transparence des flux d'informations propres aux réseaux privés.

Le nœud relais peut être considéré comme décrit par la Figure 12.

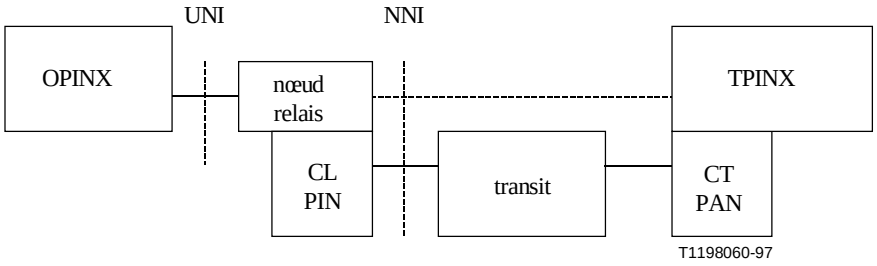


Figure 12/Q.765.1 – Illustration d'un nœud relais en interfonctionnement avec les protocoles d'interface UNI et NNI assurant ainsi l'interface entre deux fonctions de nœud PINX

7.2.4 Procédures exceptionnelles

7.2.5 Primitive d'indication d'erreur

Dès réception d'une primitive PSS1_Error contenant une notification d'erreur indiquant "non-identification de contexte" et si l'option de faire progresser les appels sans association applicative est prise en charge (voir 6.2.6), le nœud doit invoquer la capacité PINX passerelle (voir 7.2.3.2.5). Si cette option n'est pas prise en charge, l'appel doit être libéré et la fonction de gestion doit en recevoir notification.

Dès réception d'une primitive PSS1_Error contenant une notification d'erreur indiquant "erreur de réassemblage", la fonction de gestion doit en recevoir notification.

Dès réception d'une primitive PSS1_Error contenant une notification d'erreur indiquant "information non reconnue", l'appel sera si possible autorisé à progresser ou sera, sinon, libéré.

Dès réception d'une primitive PSS1_Error contenant une notification d'erreur indiquant "information obligatoire non reconnue", l'appel doit être libéré avec le code de cause 111 – Erreur de protocole, non spécifiée.

7.2.6 Contenu des primitives

Les Tableaux 6 et 7 contiennent la liste des paramètres contenus dans les primitives.

Le Tableau 8 montre le contenu de la primitive PSS1_Data envoyée en association avec les messages ISUP dans un appel VPN prenant en charge la continuité des flux informationnels PSS1.

Les indications M/O (obligatoire/facultatif) sont fournies en plus d'une référence pour une description détaillée des paramètres.

Tableau 6/Q.765.1 – Contenu de la primitive d'ind./dem. PSS1_Data

Paramètre	Obligatoire/Facultatif
Indicateurs ATII	M
Indication de transparence aux éléments de service VPN	O
Capacité de transformation en nœud PINX passerelle	O
Identificateur CNID	O
Demande de nœud PINX passerelle	O
Acquittement d'établissement	O
Numéro de l'appelant	O
Numéro de l'appelé	O
Numéro connecté	O
Fonctionnalité (Note)	O
Indicateur de notification (Note)	O
Fin de numérotation	O
Compteur de transits	O
NOTE – Ces paramètres peuvent être répétés.	

Tableau 7/Q.765.1 – Contenu de la primitive d'ind. PSS1_Error

Paramètre	Obligatoire/Facultatif
Notification d’erreur	M

Tableau 8/Q.765.1 – Contenu des primitives de dem./ind. PSS1_Data primitives envoyés en association avec des messages ISUP dans un appel VPN avec prise en charge de la continuité des flux informationnels PSS1

Message ISUP	Paramètres des primitives de dem./ind. PSS1_Data (Obligatoires/Facultatifs)
IAM	• Numéro de l'appelé (M) • Indicateurs ATII (M) • Capacité de transformation en nœud PINX passerelle (O) • Identificateur CNID (O)| • Numéro de l'appelant (O) • Fonctionnalité (O) (Note) • Indicateur de notification (O) (Note) • Fin de numérotation (O) • Compteur de transits (O)
ACM	• Indicateurs ATII (M) • Indication de transparence aux éléments de service VPN (O) • Fonctionnalité (O) (Note) • Indicateur de notification (O) (Note)
CPG	• Indicateurs ATII (M) • Indication de transparence aux éléments de service VPN (O) • Fonctionnalité (O) (Note) • Indicateur de notification (O) (Note)
ANM	• Indicateurs ATII (M) • Indication de transparence aux éléments de service VPN (O) • Numéro connecté (O) • Fonctionnalité (O) (Note) • Indicateur de notification (O) (Note)
CON	• Indicateurs ATII (M) • Indication de transparence aux éléments de service VPN (O) • Numéro connecté (O) • Fonctionnalité (O) (Note) • Indicateur de notification (O) (Note)
PRI	• Indicateurs ATII (M) • Indication de transparence aux éléments de service VPN (O) • Fonctionnalité (O) (Note) • Indicateur de notification (O) (Note)
APM	• Indicateurs ATII (M) • Numéro de l'appelé (O) • SetupAcknowledgement (O) • Indication de transparence aux éléments de service VPN (O) • Fonctionnalité (O) (Note) • Indicateur de notification (O) (Note) • Fin de numérotation (O)
NOTE – Ces paramètres peuvent être répétés.	

7.3 Fonctions du processus d'application VPN – Connexion sans communication (non associée au support)

7.3.1 Introduction

La fonction de l'aspect du processus d'application (AP) qui concerne la prise en charge des applications VPN par l'interface NNI avec le réseau public consiste à assurer la coordination entre les fonctions de processus d'application sur réseau privé (VPN) et de processus d'application sur réseau public. Lorsque l'application privée nécessite l'établissement d'une association sémaphore sans support, le processus d'application convertit les informations d'adressage privé pour leur donner la forme que le processus d'application public peut utiliser afin d'acheminer l'appel depuis le nœud public initiateur (PIN) jusqu'au commutateur approprié du réseau public (nœud public adressé, PAN) qui contient la fonction adjacente de nœud PINX. Le concept de nœuds PIN/PAN est décrit dans la référence [23]. L'utilisation de ce concept pour un réseau privé spécifique est décrite au 3.1. La conversion des informations privées en une forme appropriée à l'acheminement dans le réseau public est hors du domaine d'application de la présente Recommandation.

Celle-ci ne vise pas à redéfinir la capacité de nœud PINX dans le système PSS1. La présente Recommandation vise à décrire la façon dont, au moyen des sous-systèmes TC et SCCP, les services attendus par le système PSS1 à l'interface (définie dans la référence [3]) entre commande de transport fonctionnel générique (GFT, *generic functional transport*) et commande de protocole (PC) sont assurés dans un VPN afin de réaliser la continuité des flux informationnels PSS1 de part et d'autre de l'interface NNI avec le réseau public.

L'interface avec les primitives PSS1 entre commandes GFT et CC (voir le modèle ISO/CEI dans la référence [3]) n'est visible depuis aucune interface dans le modèle ALS. La présente Recommandation vise à ne pas modéliser le processus d'application; cependant, afin d'illustrer la relation entre la présente Recommandation et la fonction de nœud PINX définie par l'ISO, on peut utiliser la Figure 11.

La signalisation en mode sans connexion n'est pas prise en charge par la présente Recommandation.

7.3.2 Interface avec les primitives (AP-TC SACF)

L'application VPN utilise les services fournis par l'interface [(h) sur la Figure 4] avec les primitives entre AP et TC SACF, tels qu'ils sont énumérés dans le Tableau 9.

Tableau 9/Q.765.1 – Primitives entre AP et TC SACF

Nom de la primitive	Types	Sens (Note)
PSS1_Setup	Indication/Demande/ Réponse/Confirmation	→ / ← / ← / →
PSS1_Release	Indication/Demande	→ / ←
PSS1_Reject	Indication/Demande	→ / ←
PSS1_Facility	Indication/Demande	→ / ←
PSS1_SetupAck	Indication/Demande	→ / ←
NOTE – Flux de primitives de SACF vers AP: → Flux de primitives de l'AP vers SACF: ←		

7.3.3 Procédures de signalisation en mode connexion

Les procédures de commande de protocole qui décrivent le mappage des primitives de transport fonctionnel générique (GFT) avec les opérations du gestionnaire de transactions (TC) de part et d'autre de l'interface NNI avec le réseau public sont ici décrites conformément à la référence [3]. Les aspects concernant la procédure de la capacité de nœud PINX sont hors du domaine d'application de la présente Recommandation (voir 6.2.5 au sujet de la capacité offerte par le VPN). Pour décrire la relation entre les primitives à l'interface GFT/PC et les opérations utilisées par le gestionnaire TC, la présente Recommandation définit le mappage entre les primitives citées dans la référence [3] et les primitives appropriées de l'interface AP/TC SACF. Voir le Tableau 10.

Les primitives associées à la capacité d'applications privées sont hors du domaine d'application de la présente Recommandation (voir référence [3]).

Tableau 10/Q.765.1 – Mappages entre primitives utilisées dans la référence [3] et primitives AP/TC SACF

COLONNE A Primitives utilisées à l'interface GFT/PC définie dans la référence [3]	COLONNE B Primitives utilisées à l'interface AP/TC SACF
PC_SETUP demande/indication	PSS1_SETUP demande/indication
PC_SETUP réponse/confirmation	PSS1_SETUP réponse/confirmation
PC_RELEASE demande/indication	PSS1_RELEASE demande/indication
PC_REJECT demande/indication	PSS1_REJECT demande/indication
PC_DATA demande/indication	PSS1_FACILITY demande/indication
(non applicable)	PSS1_SetupAck demande/indication

7.3.3.1 Identificateur de réseau de télécommunication d'entreprise

L'identificateur de réseau de télécommunication d'entreprise (CNID) est soit fourni par l'accès entrant de l'interface usager-réseau (UNI) soit par une valeur implicitement liée à l'accès entrant. L'identificateur CNID n'est requis que pour l'établissement d'appels [opération SETUP (TC)] et est obligatoire de part et d'autre de l'interface internationale car il a une portée mondiale. L'emploi d'un autre mécanisme d'identification d'un réseau de télécommunication d'entreprise relève d'une option de l'opérateur de réseau, dans son propre domaine. Dès réception d'un identificateur CNID non reconnu par le nœud PAN, la connexion doit être libérée avec la cause 63 (service ou option indisponible – non spécifiée) et la fonction de gestion doit en recevoir notification.

7.3.3.2 Nœud relais

Voir 7.2.3.4.

7.3.4 Contenu des primitives

Les Tableaux 11 à 15 contiennent la liste des paramètres insérés dans les primitives.

La primitive PSS1_SetupAck ne contient pas de paramètres.

Les indications M/O (obligatoire/facultatif) sont fournies en plus d'une référence pour une description détaillée des paramètres.

Tableau 11/Q.765.1 – Contenu de la primitive d'ind./dem. PSS1_SETUP

Paramètre	Obligatoire/Facultatif
Numéro public de l'appelé	M
Numéro de l'appelé	M
Numéro de l'appelant	O
Identificateur de réseau de télécommunication d'entreprise	O
Fonctionnalité (Note)	O
Compteur de transits	O
NOTE – Ces paramètres peuvent être répétés.	

Tableau 12/Q.765.1 – Contenu de la primitive de rép./conf. PSS1_SETUP

Paramètre	Obligatoire/Facultatif
Numéro connecté	O
Fonctionnalité (Note)	O
NOTE – Ces paramètres peuvent être répétés.	

Tableau 13/Q.765.1 – Contenu de la primitive d'ind./dem. PSS1_RELEASE

Paramètre	Obligatoire/Facultatif
Cause	M
Fonctionnalité (Note)	O
NOTE – Ces paramètres peuvent être répétés.	

Tableau 14/Q.765.1 – Contenu de la primitive d'ind./dem. PSS1_REJECT

Paramètre	Obligatoire/Facultatif
Cause	M
Fonctionnalité (Note)	O
NOTE – Ces paramètres peuvent être répétés.	

Tableau 15/Q.765.1 – Contenu de la primitive d'ind./dem. PSS1_FACILITY

Paramètre	Obligatoire/Facultatif
Fonctionnalité (Note)	M
NOTE – Ces paramètres peuvent être répétés.	

8 Fonction de contrôle d'association unique (SACF) – SUP SACF

8.1 Introduction

Le principal objet de la fonction ISUP SACF est de recevoir/émettre des primitives à destination et en provenance de l'entité appropriée ainsi que d'assurer, le cas échéant, une fonction de distribution pour l'invocation ISUP AEI. Le flux d'informations va du processus d'application [interface (a) sur la Figure 4] à [l'interface (f) sur la Figure 4] NI ou inversement. La fonction SACF est donc également chargée de faire en sorte que, lorsque les éléments ASE émettent des primitives multiples vers le processus d'application, ces primitives soient acheminées ensemble de part et d'autre de l'interface, afin que les associations correctes soient conservées. La fonction SACF ici décrite ne définit que les mappages et fonctions associés à la partie du modèle qui concerne la prise en charge des applications VPN par l'interface NNI. Le rôle de la fonction SACF par rapport au mécanisme APM sur réseau public est hors du domaine d'application de la présente Recommandation. Les mappages entre primitives indiqués dans les Tableaux 16 et 19 sont décrits dans la référence [23] et ne sont reproduits ici qu'à titre documentaire.

Les interfaces citées ici sont illustrées dans la Figure 4 du 6.2. Des exemples de "flux dynamiques de primitives" sont décrits au 6.2.3.

Les primitives à l'interface (a) entre fonction SACF et processus AP sont définies au 7.2.2.

Les paramètres contenus dans ces primitives sont énumérés dans les Tableaux 6 à 8.

Les primitives à l'interface (b) entre fonction SACF et éléments PSS1 ASE sont définis dans le 10.1.

Les paramètres contenus dans ces primitives sont énumérés dans les Tableaux 24 à 25.

Les primitives à l'interface (c) entre fonction SACF et éléments UCEH ASE sont définis dans la référence [23] et sont donc hors du domaine d'application de la présente Recommandation.

Les primitives à l'interface (d) entre fonction SACF et éléments APM ASE sont définis dans la référence [23] et sont donc hors du domaine d'application de la présente Recommandation.

Les primitives à l'interface (e) entre fonction SACF et élément ISUP ASE sont définis dans la référence [23] et sont donc hors du domaine d'application de la présente Recommandation.

Les primitives à l'interface (f) entre fonction SACF et interface NI sont définis dans la référence [23] et sont donc hors du domaine d'application de la présente Recommandation.

8.2 Flux informationnels relatifs aux messages envoyés par le nœud

Dès réception d'une primitive (demande ou réponse) issue du processus d'application [interface (a) de la Figure 4], la fonction SACF envoie aux éléments ASE la ou les primitives appropriées, après avoir inséré les paramètres dans les primitives ainsi créées à partir du sous-ensemble approprié des paramètres reçus du processus d'application. La fonction SACF assure également la distribution des primitives de réponse reçues des éléments ASE avant d'envoyer la primitive résultante à [l'interface (f) sur la Figure 4] NI.

Tableau 16/Q.765.1 – Mappages entre primitives PSS1 ASE et primitives APM ASE

Interface (b), en prov enance des éléments PSS1 ASE	Interface (d), APM ASE
APM_U_Data	APM_Data

Tableau 17/Q.765.1 – Mappages entre primitives AP et PSS1 ASE

Interface (a), en provenance du processus AP	Interface (b), PSS1 ASE
PSS1_Data	PSS1_Data

8.3 Flux informationnels relatifs aux messages reçus par le nœud

Ces procédures sont décrites dans la référence [23], où l'élément ASE d'utilisateur APM correspond à l'élément PSS1 ASE.

Tableau 18/Q.765.1 – Mappages entre primitives PSS1 ASE et primitives AP

Interface (b), PSS1 ASE	Interface (a), en provenance du processus AP
PSS1_Data	PSS1_Data
PSS1_Error	PSS1_Error

Tableau 19/Q.765.1 – Mappages entre primitives APM ASE et PSS1 ASE

Interface (d), en provenance des éléments APM ASE	Interface (b), PSS1 ASE
APM_Data	APM_U_Data

Tableau 20/Q.765.1 – Mappages entre primitives UCEH ASE et PSS1 ASE

Interface (c), en provenance des éléments UCEH ASE	Interface (b), PSS1 ASE
APM_Error	APM_U_Error

9 Fonction de contrôle d'association unique (SACF) – TC SACF

9.1 Introduction

Le principal objectif de la fonction TC SACF est de recevoir/émettre des primitives à destination et en provenance de l'entité appropriée pour les invocations TC AEI. La fonction SACF décrite ici ne définit que les mappages et les fonctions associés à la prise en charge de la partie du modèle qui concerne les applications VPN.

Quatre interfaces (représentées sur la Figure 4) sont décrites par la présente Recommandation:

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

Les interfaces mentionnées ici sont illustrées à la Figure 4 du 6.2. Le sous-paragraphe 6.2.3 donne également des exemples des "flux dynamiques de primitives".

Les primitives reçues du processus AP à l'interface (h) sont mappées comme indiqué dans les 7.3.2 et 7.4.2. Les paramètres contenus dans ces primitives sont énumérés au 7.3.5.

Les primitives à l'interface (i) entre fonction SACF et éléments COPSS1 ASE sont énumérées au 11.1.

Les primitives à l'interface (j) entre fonction SACF et sous-système TCAP sont énumérées dans les références [16] à [20] (voir le paragraphe 12).

Les primitives à l'interface (k) entre fonction SACF et sous-système SCCP sont énumérées dans les références [7] à [12] (voir le paragraphe 13).

9.2 Flux informationnels relatifs aux messages envoyés par le nœud

Dès réception d'une primitive (demande ou réponse) issue du processus d'application [interface (h) de la Figure 4], la fonction SACF envoie aux éléments ASE la ou les primitives appropriées, après avoir inséré les paramètres dans les primitives ainsi créées à partir du sous-ensemble approprié des paramètres reçus du processus d'application. La fonction SACF assure également la distribution des primitives de réponse reçues des éléments ASE avant d'envoyer la primitive résultante. Concernant l'interface entre fonction SACF et sous-système TCAP, toutes les primitives TC échangées entre les éléments COPSS1 ASE et le sous-système TCAP passent par la fonction SACF en transparence. Voir le Tableau 21.

Tableau 21/Q.765.1 – Mappages entre primitives AP et éléments COPSS1 ASE

Interface (h), en provenance du processus 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 Flux informationnels relatifs aux messages reçus par le nœud

Dès réception d'une primitive d'indication N_DATA issue du sous-système SCCP, la fonction SACF analyse le champ de données d'utilisateur contenu dans cette primitive, conformément aux règles indiquées dans la référence [9]. Il procède ensuite à l'exécution de la fonction de distribution. Voir le Tableau 22.

Tableau 22/Q.765.1 – Mappages entre primitives COPSS1 ASE et primitives AP

Interface (i), COPSS1 ASE	Interface (h), en provenance du processus AP
PSS1_Setup	PSS1_Setup
PSS1_SetupAck	PSS1_SetupAck
PSS1_Release	PSS1_Release
PSS1_Reject	PSS1_Reject
PSS1_Facility	PSS1_Facility

10 Elément ASE du système PSS1 (PSS1 ASE)

L'élément ASE du système PSS1 est chargé des fonctions de signalisation de l'application VPN pour la prise en charge des flux informationnels PSS1 et pour la préparation des informations sous une forme appropriée à leur communication au mécanisme APM en vue de leur transport.

10.1 Interface avec les primitives

Le Tableau 23 énumère les primitives à [l'interface (b) sur la Figure 4] entre éléments PSS1 ASE et fonction ISUP SACF.

Tableau 23/Q.765.1 – Primitives entre fonction ISUP SACF et éléments PSS1 ASE (APM)

Nom de la primitive	Types	Sens (Note)
APM_U_Data	Indication/Demande	→ / ←
APM_U_Error	Indication	→
PSS1_Error	Indication	→
PSS1_Data	Indication/Demande	→ / ←
NOTE – Flux de primitives de la fonction SACF vers des éléments PSS1 ASE: → Flux de primitives des éléments PSS1 ASE vers la fonction SACF: ←		

10.2 Procédures de signalisation

10.2.1 Nœud public initiateur

10.2.1.1 Procédures d'émission

Dès réception de la primitive de demande PSS1_Data, son contenu est converti dans le format approprié (voir le paragraphe 14) et la valeur d'identificateur de contexte est mise à "élément PSS1 ASE (VPN)". Le résultat est envoyé dans la primitive de demande APM_U_Data.

10.2.1.2 Procédures de réception

Dès réception de la primitive d'indication APM_U_Data, son contenu est vérifié en termes d'exactitude de formatage et de codage (voir le paragraphe 14). Si cette vérification est satisfaisante, les informations reçues sont transférées et envoyées dans la primitive d'indication PSS1_Data. Si la vérification n'est pas satisfaisante, la même primitive d'indication PSS1_Error est envoyée avec les résultats et l'indication "informations non reconnues". Si une valeur non reconnue est reçue pour le champ indicateur d'identificateur CNID, la notification d'erreur envoyée dans la primitive d'indication PSS1_Error doit indiquer "information obligatoire non reconnue".

10.2.1.3 Primitive APM_U_Error

Dès réception de la primitive d'indication APM_U_Error, le contenu doit être transmis sans changement dans la primitive PSS1_Error.

10.2.2 Nœud public adressé

Voir 10.2.1.

10.2.3 Encombrement de signalisation

Pour éviter un encombrement dans le réseau de signalisation n° 7, il est nécessaire que les applications contribuant à la charge sémaphore vers une destination encombrée limitent de manière régulière leur trafic sémaphore. Au fur et à mesure que le processus d'application fait usage des éléments ISUP ASE, la procédure ISUP de réduction des encombrements de signalisation [14] peut diminuer le trafic vers une destination affectée. Dans ce cas, les nouvelles tentatives d'appel peuvent être provisoirement rejetées.

10.3 Contenu des primitives

Les Tableaux 24 et 25 énumèrent les contenus obligatoires et facultatifs des primitives de service pour les éléments PSS1 ASE. Ces primitives sont définies dans la référence [23] et ne sont présentées ici qu'à titre documentaire.

Le contenu des primitives PSS1_Error et PSS1_Data est défini au 7.2.6 pour l'interface AP/SACF.

Les indications M/O (obligatoire/facultatif) sont fournies.

Tableau 24/Q.765.1 – Contenu de la primitive d'ind./dem. APM_U_Data

Paramètre	Obligatoire/Facultatif
Identificateur de contexte d'application	M
Indicateurs d'instruction de transport d'application	M
Données d'application	M

Tableau 25/Q.765.1 – Contenu de la primitive d'ind. APM_U_Error

Paramètre	Obligatoire/Facultatif
Notification	M

11 Elément ASE de système PSS1 en mode connexion (COPSS1 ASE)

Cet élément COPSS1 ASE est chargé des aspects de signalisation de l'application VPN pour la prise en charge des flux informationnels PSS1 ainsi que pour la préparation des informations sous la forme appropriée qui peut être transmise au gestionnaire TC pour le transport.

11.1 Séquence d'utilisateur TC

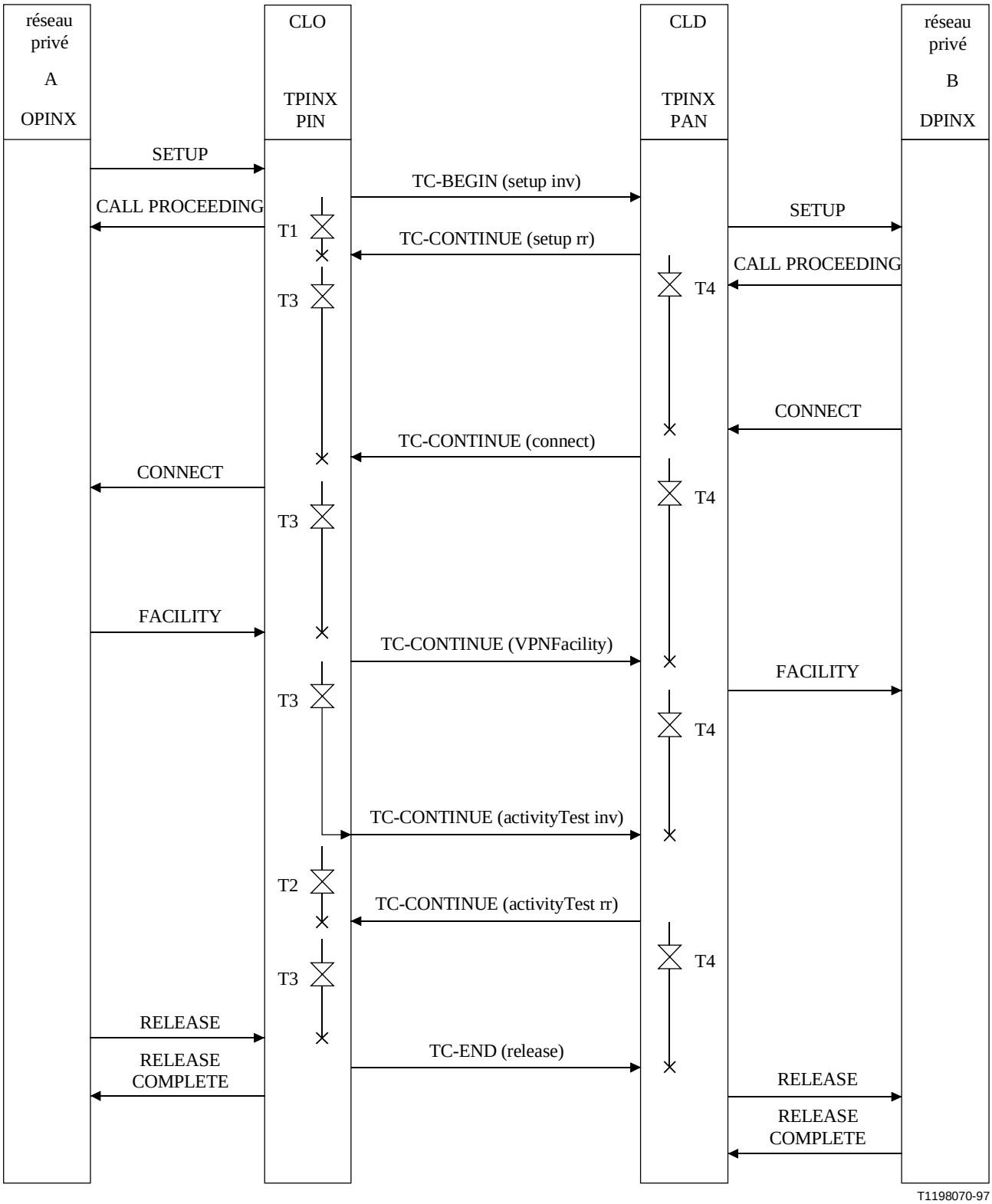
Flux de signalisation pour établissement et libération d'appel

Dans la Figure 13, un flux de signalisation est indiqué pour les opérations d'établissement et de libération d'un dialogue afin de prendre en charge le transfert d'informations par réseau privé sans association avec un support (en mode connexion). Les éléments d'informations de l'interface UNI sont transférés par l'interface NNI au moyen de messages TC. Les opérations suivantes sont définies pour permettre le transfert des flux informationnels UNI correspondants: ***Setup, Connect, Release, VpnFacility***. L'opération d'établissement est de la classe 3 et les autres opérations de la classe 4.

Deux temporisateurs supervisent la libération du dialogue avec le gestionnaire TC. Le temporisateur T3 doit être armé dans le nœud PIN dès réception de l'opération de retour de résultat d'établissement et le temporisateur T4 doit être armé dans le nœud PAN dès l'envoi de l'opération de retour de résultat d'établissement. Ces deux temporisateurs sont réarmés à chaque envoi/réception d'une opération.

Une opération de classe 3, appelée ***ActivityTest***, est envoyée pour vérifier si l'application distante est encore active. Cette opération doit être effectuée dans le nœud PIN dès l'expiration de la temporisation T3. Le temporisateur T2 doit superviser la réception du retour de résultat. Dès réception de l'opération de test d'activité, le nœud PAN doit réarmer le temporisateur T4 et, dès réception du retour de résultat, le nœud PIN doit arrêter le temporisateur T2 et armer le temporisateur T3.

A l'expiration de la temporisation T1, T2 ou T4, le nœud PIN doit envoyer une primitive TC-U-ABORT (abandon du dialogue) et en informer la fonction de gestion.



CLO: commutateur local d'origine CLD: commutateur local de destination

Figure 13/Q.765.1 – Exemple de séquence de signalisation sans association avec un support

11.2 Interface entre éléments COPSS1 ASE et fonction SACF

Le Tableau 26 énumère les primitives à l'interface entre éléments COPSS1 ASE et fonction TC SACF [interface (i) dans la Figure 4].

D'autres primitives de cette interface correspondent à l'interface avec l'utilisateur TC, telle que définie dans les références [16] et [17].

Tableau 26/Q.765.1 – Primitives entre éléments COPSS1 ASE et fonction TC SACF (commande de protocole)

Nom de la primitive	Types	Sens (Note)	Opération(s) correspondante(s)
PSS1_SETUP	Indication/Demande	→ / ←	Setup.Invoke
PSS1_SETUP	Réponse/Confirmation	← / →	Connect.Invoke
PSS1_REJECT	Indication/Demande	→ / ←	Setup.ReturnResult
PSS1_SETUPACK	Indication/Demande	→ / ←	Setup.ReturnResult
PSS1_FACILITY	Indication/Demande	→ / ←	VpnFacility.Invoke
PSS1_RELEASE	Indication/Demande	→ / ←	Release.Invoke
NOTE – Flux de primitives de SACF to COPSS1 ASE: → Flux de primitives de COPSS1 ASE to SACF: ←			

11.3 Opérations prises en charge

L'élément ASE prend en charge les opérations suivantes:

- Setup (Classe 3).
- Connect (Classe 4).
- VpnFacility (Classe 4).
- Release (Classe 4).
- ActivityTest (Classe 3).

L'invocation des opérations susmentionnées peut produire les composants suivants:

- Setup
  - Setup. Invoke
  - Setup.ReturnResult
- Connect
  - Connect.Invoke
- VpnFacility
  - VpnFacility.Invoke
- Release
  - Release.Invoke
- ActivityTest
  - ActivityTest.Invoke
  - ActivityTest.ReturnResult

11.4 Procédures pour les éléments ASE

L'élément COPSS1 ASE est chargé de la coordination des informations reçues dans les primitives et de leur préparation conformément à la définition des opérations et aux prescriptions applicables à l'interface avec les primitives du sous-système TCAP.

11.4.1 Relation entre l'élément COPSS1 ASE et le sous-système TCAP

Le dialogue défini pour la prise en charge des flux d'information PSS1 entre entités homologues (Utilisateurs TC) est structuré. Le paramètre d'identification de dialogue est utilisé dans les deux primitives de traitement d'opération et de traitement de transmission (dialogue) afin de déterminer le ou les composants qui se rapportent à chaque dialogue.

Chaque utilisateur TC possède sa propre référence pour un dialogue donné. Ces références sont locales et leur mappage avec les identificateurs de transaction concernant les références de protocole, insérés dans les messages, est effectué par le gestionnaire TC.

Toutes les opérations ci-dessous appartiennent au même dialogue.

Les opérations des classes 3 et 4 sont utilisées.

Chaque message TC n'achemine qu'une seule opération.

11.4.1.1 Début du dialogue

Le nœud PIN ouvre le dialogue en utilisant une primitive de demande TC-BEGIN avec une primitive de demande TC_INVOKE afin de transmettre au nœud PAN un composant d'invocation d'opération d'établissement (classe 3). Ce nœud PAN répond comme suit:

- en utilisant la primitive de demande TC-CONTINUE avec la primitive de demande TC-RESULT-L afin de transmettre un composant Setup.ReturnResult, de confirmer le dialogue et d'indiquer que l'opération de demande d'établissement a été efficace. Dans ce cas, aucun paramètre n'est inséré dans le résultat Setup.ReturnResult;
- en utilisant la primitive de demande TC-END avec la primitive de demande TC-RESULT afin de transmettre un composant Setup.ReturnResult, de mettre fin au dialogue et d'indiquer que l'opération de demande d'établissement n'a pas été efficace. Dans ce cas, le paramètre de cause doit être inclus. De plus, un ou plusieurs éléments d'information "Extensions de couche Réseau" peuvent être insérés dans le paramètre VPNTransport.

11.4.1.2 Poursuite du dialogue

La poursuite du dialogue est assurée par les opérations Connect (classe 4), VpnFacility (classe 4) et ActivityTest (classe 3) au moyen des primitives de type TC-CONTINUE.

11.4.1.3 Fin du dialogue

11.4.1.3.1 Fin normale

Une fin de dialogue est demandée par le nœud PIN ou PAN au moyen d'une primitive de demande TC_END avec une primitive de demande TC-INVOKE pour transmettre un composant d'invocation d'opération de libération.

11.4.1.3.2 Fin anormale

Lorsque l'utilisateur TC détermine qu'il va abandonner le dialogue, il procède à cette opération au moyen de la primitive TC-U-ABORT. Dès réception d'une primitive d'indication TC-NOTICE ou TC-P-ABORT, le dialogue avec le gestionnaire TC doit être arrêté.

11.4.2 Opérations

11.4.2.1 Opération d'établissement

Dès réception de la primitive de demande PSS1_SETUP, son contenu est chargé dans le nœud PIN et envoyé par celui-ci avec l'opération Setup.invoke. Le temporisateur T1 est armé. Dès réception de cette demande d'opération dans le nœud PAN, son contenu est envoyé dans une primitive d'indication PSS1_SETUP. Si la demande de connexion sémaphore peut être acceptée par le processus d'application au nœud PAN (l'élément COPSS1 ASE reçoit une demande PSS1_SETUPACK), ce nœud renvoie en réponse au nœud PIN l'opération Setup.ReturnResult et arme le temporisateur T4. Dès réception de l'opération de retour de résultat au nœud PIN, son contenu est envoyé dans une indication PSS1_SETUPACK, le temporisateur T1 est arrêté et le temporisateur T3 est armé. Si la demande de connexion sémaphore ne peut pas être acceptée par le processus d'application au nœud PAN (l'élément COPSS1 ASE reçoit une demande PSS1_REJECT), ce nœud renvoie l'opération Setup.ReturnResult en réponse au nœud PIN qui, dès qu'il la reçoit, en envoie le contenu dans une indication PSS1_REJECT et arrête le temporisateur T1.

11.4.2.2 Opération de connexion

Dès réception de la première primitive de réponse PSS1_SETUP, son contenu est chargé dans le nœud PAN et envoyé par celui-ci avec l'opération Connect.invoke. Le temporisateur T4 est réarmé. Dès réception de cette opération par le nœud PIN, celui-ci en transmet le contenu dans la primitive de confirmation PSS1_SETUP et le temporisateur T3 est réarmé.

11.4.2.3 Opération VpnFacility

L'opération VpnFacility peut être envoyée par le nœud PIN vers le nœud PAN ou inversement, après envoi/réception de l'opération Connect.invoke.

Dans le sens PIN vers PAN: dès réception de la primitive de demande PSS1_FACILITY, son contenu est chargé dans le nœud PIN et envoyé par celui-ci avec l'opération VpnFacility.invoke. Le temporisateur T3 est réarmé. Dès réception de l'opération au nœud PAN, son contenu est transmis dans la primitive d'indication PSS1_FACILITY et le temporisateur T4 est réarmé.

Dans le sens PAN vers PIN: dès réception de la primitive de demande PSS1_FACILITY, son contenu est chargé dans le nœud PAN et envoyé par celui-ci avec l'opération VpnFacility.invoke. Le temporisateur T4 est réarmé. Dès réception de l'opération au nœud PIN, son contenu est transmis dans la primitive d'indication PSS1_FACILITY et le temporisateur T3 est réarmé.

11.4.2.4 Opération ActivityTest

A l'expiration de la temporisation T3, le nœud PIN envoie une opération ActivityTest.invoke et arme le temporisateur T2. Dès réception de l'opération, le nœud PAN envoie l'opération ActivityTest.returnresult en réponse et réarme le temporisateur T4. Dès réception de la réponse dans le nœud PIN, le temporisateur T2 est arrêté et le temporisateur T3 est armé.

11.4.2.5 Opération de libération

L'opération de libération peut être envoyée par le nœud PIN vers le nœud PAN ou inversement.

Dans le sens PIN vers PAN: dès réception de la primitive de demande PSS1_RELEASE, son contenu est chargé dans le nœud PIN et envoyé par celui-ci avec l'opération Release.invoke. Le temporisateur T3 est arrêté. Dès réception de l'opération au nœud PAN, son contenu est transmis dans la primitive d'indication PSS1_RELEASE et le temporisateur T4 est arrêté.

Dans le sens PAN vers PIN: dès réception de la primitive de demande PSS1_RELEASE, son contenu est chargé dans le nœud PAN et envoyé par celui-ci avec l'opération Release.invoke. Le temporisateur T4 est arrêté. Dès réception de l'opération au nœud PIN, son contenu est transmis dans la primitive d'indication PSS1_RELEASE et le temporisateur T3 est arrêté.

11.4.2.6 Procédures exceptionnelles

Dès réception d'une primitive TC-P-ABORT, TC-U-ABORT, TC-U-REJECT, TC-L-CANCEL ou TC-NOTICE, le dialogue est libéré avec la cause "normale non spécifiée".

11.4.3 Expiration des temporisateurs

11.4.3.1 Temporisateur T1

A l'expiration de la temporisation T1, le dialogue doit être libéré au moyen de la primitive TC-U-ABORT et la primitive d'indication PSS1_REJECT doit être envoyée au processus d'application avec la cause "normale non spécifiée".

11.4.3.2 Temporisateur T2

A l'expiration de la temporisation T2, le dialogue doit être libéré au moyen de la primitive TC-U-ABORT et la primitive d'indication PSS1_RELEASE doit être envoyée au processus d'application avec la cause "normale non spécifiée".

11.4.3.3 Temporisateur T3

A l'expiration de la temporisation T3, les procédures de test d'activité doivent être lancées (voir 11.4.2.4).

11.4.3.4 Temporisateur T4

A l'expiration de la temporisation T4, le dialogue doit être libéré au moyen de la primitive TC-U-ABORT et la primitive d'indication PSS1_RELEASE doit être envoyée au processus d'application avec la cause "normale non spécifiée".

11.4.4 Encombrement de signalisation

Pour éviter un encombrement dans le réseau de signalisation n° 7, il est nécessaire que les applications contribuant à la charge sémaphore vers une destination encombrée limitent de manière régulière leur trafic sémaphore. Au fur et à mesure que le processus d'application fait usage des éléments ISUP ASE, les éléments COPSS1 ASE doivent prendre les mesures nécessaires dès réception d'une primitive TC NOTICE indiquant un encombrement de signalisation. Comme dans le cas des procédures ISUP de réduction des encombrements de signalisation [14], il y a lieu que le processus d'application réduise le nombre des établissements de nouvelles transactions vers la destination affectée.

11.5 Contenu des primitives

Le contenu des primitives est décrit au 7.3.4.

11.6 Syntaxe abstraite – Définition générale

Le sous-paragraphe 11.8 spécifie en notation ASN.1 la syntaxe abstraite applicable au protocole des éléments COPSS1 ASE [25].

L'ensemble des valeurs dont chacune correspond à un type de message TCAP en notation ASN.1 défini dans les références [16] à [20] (les définitions de type ANY DEFINED BY étant résolues par les définitions d'opérations et d'erreurs figurant au 11.8) constitue la syntaxe abstraite pour le protocole des éléments COPSS1 ASE.

L'ensemble des règles de codage applicables à cette syntaxe abstraite est défini par les références [16] à [20]. Le mappage des macros de type OPERATION et ERROR avec les composants du sous-système TC est également décrit dans les références [16] à [20].

Le type de données ASN.1 qui suit les mots clés "PARAMETER" ou "RESULT" (pour les macros OPERATION et ERROR) est toujours facultatif du point de vue syntaxique. Cependant, sauf indication expresse, ce type doit être considéré comme obligatoire du point de vue sémantique.

Lorsqu'un élément obligatoire fait défaut dans un composant ou dans une structure interne de données, un composant de rejet est renvoyé (si le dialogue est toujours ouvert). La cause du problème à invoquer est "erreur de type de paramètre".

11.7 Numéro de sous-système

La valeur de numéro SSN 0000 1011 ("services complémentaires RNIS") sera utilisée.

11.8 Module ASN.1

Le module ASN.1 suivant spécifie les éléments de protocole définis pour les éléments COPSS1 ASE. Il montre la définition des opérations, des erreurs et des types requis pour la signalisation sans association au support en mode connexion afin de prendre en charge les flux informationnels PSS1 au moyen de la notation ASN.1 comme indiqué dans la référence [25] et au moyen des macros OPERATION et ERROR définies par les références [16] à [20].

La définition formelle des types de composants nécessaires pour coder ces opérations, erreurs et types est indiquée dans les références [16] à [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)};

================================================================================
-- DÉFINITIONS DES TYPES POUR LES OPÉRATIONS
================================================================================

-- Spécification de l'opération Setup
-- ==========================

-- Sens:        CLO → CLD

-- Classe:      3

-- Temporisateur:     T1

-- Objet:       opération utilisée pour l'établissement d'une association sémaphore entre un nœud PIN et un nœud PAN
pour une connexion sémaphore sans association avec un support.
```

SetUp **::= OPERATION**

ARGUMENT

SetUpArg

RESULT

SetUpResultArg

-- Spécification de l'opération Connect

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

-- Sens: CLD → CLO

-- Classe: 4

-- Objet: indique que la connexion sémaphore a atteint l'état actif.

Connect **::= OPERATION**

ARGUMENT

ConnectArg

-- Spécification de l'opération Release

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

-- Sens: CLO → CLD et CLD → CLO

-- Classe: 4

-- Objet: opération utilisée pour libérer une association sémaphore entre un nœud PIN et un nœud PAN.

Release **::= OPERATION**

ARGUMENT

ReleaseArg

-- Spécification de l'opération VpnFacility

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

-- Sens: CLO → CLD et CLD → CLO

-- Classe: 4

-- Objet: opération utilisée pour transporter des flux informationnels PSS1 au cours de la phase active d'une connexion sémaphore.

VpnFacility **::= OPERATION**

ARGUMENT

VpnFacilityArg

-- Spécification de l'opération ActivityTest

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

-- Sens: CLO → CLD

-- Classe: 3

-- Temporisateurr: T2

-- Objet: opération utilisée pour déterminer si l'association sémaphore reste établie entre un nœud PIN et un nœud PAN.

ActivityTest ::= OPERATION

RESULT

```
================================================================================
-- DÉFINITIONS DE TYPE POUR LES ERREURS
================================================================================

-
================================================================================
-- DÉFINITIONS DE TYPE POUR LES DONNÉES D'ARGUMENT
================================================================================
```

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
================================================================================
-- DÉFINITIONS DE TYPE POUR LES DONNÉES
================================================================================
CalledPartyNumber       ::= OCTET STRING (SIZE (1..maxcdPlength))
        -- Le numéro de l'appelé est codé comme indiqué dans la Recommandation Q.763 [13].
        -- Les octets du nom et de la longueur du paramètre ISUP ne sont pas inclus.

VPNTransport            ::= OCTET STRING (SIZE (0..maxLength))
        -- Le composant VPNTransport est codé comme décrit dans le paragraphe 14/Q.765.1.

Cause                   ::= OCTET STRING (SIZE (1..maxCauseLength))
        -- Le composant Cause est codé comme décrit dans l'ISO/CEI 11572 [2]/  Q.931 Annexe M [21]
        -- Les octets de l'identificateur de l'élément d'information et de sa longueur ne sont pas inclus.
.
================================================================================
-- DÉFINITION DES CONSTANTES DE LONGUEUR
================================================================================
maxCauseLength          INTEGER         ::= 30
maxLength               INTEGER         ::= 2048
maxcdPlength            INTEGER         ::= Network specific
================================================================================
-- DÉFINITION DE L'ARC D'IDENTIFICATEUR D'OBJETS
================================================================================
COPSS1OID       OBJECT IDENTIFIER    ::= {itu-t Recommendation q 765 1 operations-and-errors(1)}
================================================================================
-- ATTRIBUTIONS DES VALEURS D'OPÉRATION
================================================================================
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)}


================================================================================
-- ATTRIBUTIONS DES VALEURS D'ERREUR
================================================================================

-
```

END – *du protocole COPSS1*

12 Sous-système TCAP (TC ASE)

La fonction SACF utilise les services fournis par l'interface avec les primitives du sous-système TCAP, dont la définition est hors du domaine d'application de la présente Recommandation. Pour plus de détails, voir les références [16] à [20].

12.1 Interface entre TCAP et SACF

12.1.1 Primitives

Les primitives qui prennent en charge les services offerts par le sous-système TCAP à cette interface sont définies dans les références [16] à [20].

12.1.2 Utilisation du sous-système TCAP

Cette application utilise le sous-système TCAP pour les dialogues structurés.

Le dialogue ouvert par les éléments COPSS1 ASE entre entités homologues (Utilisateurs TC) est structuré. Le paramètre d'identification de dialogue est utilisé dans les deux primitives de traitement d'opération et de traitement de transmission (dialogue) afin de déterminer le ou les composants qui se rapportent à chaque dialogue. Chaque utilisateur TC possède sa propre référence pour un dialogue donné. Ces références sont locales et leur mappage avec les identificateurs de transaction concernant les références de protocole, insérés dans les messages, est effectué par le sous-système TCAP. La classe utilisée par chaque opération est définie en notation ASN.1.

13 Sous-système SCCP

13.1 Interface entre SCCP et SACF

La fonction TC SACF utilise les services fournis par l'interface avec les primitives du sous-système SCCP, dont la définition est hors du domaine d'application de la présente Recommandation. Pour plus de détails sur le sous-système SCCP, voir les références [7] à [12].

13.2 Utilisation du sous-système TCAP

- le service SCCP de classe 1 (service séquentiel sans connexion) est utilisé par cette application;
- l'option de renvoi des messages SCCP est toujours utilisée;
- la version 1992 du SCCP doit au minimum être utilisée mais il est préférable de faire appel à la version 1996/97 du SCCP [7] à [12].

13.3 Routage dans le réseau SCCP

Pour le routage à l'interface internationale et le routage fondé sur le mécanisme de conversion des titres globaux dans les réseaux nationaux, le codage de l'adresse de l'appelé et de l'appelant dans le SCCP doit être conforme aux restrictions suivantes:

indicateur de numéro SSN	1	(le numéro SSN pour les services complémentaires du RNIS est toujours inclus)
indicateur de titre global	0100	(cet indicateur comporte le système de codage du plan de numérotage et la nature de l'adresse pour le type de conversion)
type de conversion	0001 0001	(table de conversion)
plan de numérotage	0001	(plan de numérotage E.164 pour RNIS/téléphonie)
indicateur de routage	0	(routage selon le titre global)

En variante, pour le routage à l'intérieur d'un réseau national, la méthode d'adressage du SCCP, fondée sur des commandes SPC, peut s'appliquer. Cependant, à l'intérieur de grands réseaux nationaux, il serait préférable d'utiliser une méthode d'adressage hybride, fondée sur des commandes SPC pour le trafic régional et sur un mécanisme de conversion de titre global pour le trafic à grande distance, afin de conserver des données de routage SS n° 7 maniables.

13.4 Informations numériques utilisées pour le routage

Le commutateur qui ouvre un dialogue utilisant le mécanisme de conversion de titre global doit indiquer une adresse E.164 comme GT dans le champ SCCP d'adresse de l'appelant, cette adresse identifiant ce titre de façon unique. Pour le routage par une interface internationale, les informations numériques utilisées pour la conversion du titre global doivent être conformes aux plans de numérotage E.164 pour ce qui est de l'indicatif de pays et de l'indication national de destination.

14 Transport par le VPN – Formats et codes des données d'application

Les formats et codes des données d'application VPN pour la prise en charge des flux informationnels PSS1 sous forme d'utilisateurs APM sont définis ci-après. La structure des informations ici définie est transmise en tant que "données d'application" au mécanisme de transport sous-jacent (APM) dans la primitive APM_U_Data. Le champ d'identificateur de contexte d'application du paramètre de transport d'application (APP) doit être codé à la valeur "Elément PSS1 ASE (VPN)".

Le champ d'informations d'applications encapsulé dans le paramètre APP est codé comme le composant VPNTransport. Le format de ce champ est tel qu'il puisse fournir un service de transport transparent d'informations (voir 14.1) et qu'il possède la capacité de transmettre dans le réseau public des informations additionnelles associées au réseau (voir 14.2). Les informations d'application sont structurées de façon que le premier octet soit un pointeur sur les informations à transporter en transparence (voir 14.1). La valeur (binaire) du pointeur donne le nombre d'octets compris entre l'octet pointeur (inclus) et le premier octet (non inclus) des données PSS1 transparentes. La valeur zéro du pointeur sert à indiquer qu'il n'y a pas de données PSS1 transparentes. L'étendue des octets compris entre l'octet pointeur et le premier octet de données PSS1 transparentes (sur lequel pointe l'octet pointeur) contient les informations de couche Réseau (voir 14.2) à transmettre entre les applications VPN résidant dans le réseau public.

14.1 Eléments d'information propres aux réseaux privés, à transporter dans le paramètre de transport d'application

Le transport transparent de flux informationnels PSS1 par le paramètre APP est réalisé par l'acheminement des éléments d'information énumérés dans le Tableau 27.

Tableau 27/Q.765.1 – Eléments d'information transportés dans le paramètre APP

Elément d'information	Réf.	Type	Longueur
Numéro de l'appelant	[2]/[21] (Note 1)	O	4-*
Numéro de l'appelé	[2]/[21](Note 1)	O	4-*
Numéro connecté	[2]/[21](Note 1)	O	4-*
Fonctionnalité avec valeur de profil de protocole mise à "Extensions de réseautage" (Note 2)	[3]/[22](Note 1)	O	3-*
Indicateur de notification (Note 2)	[3]/[22](Note 1)	O	3-*
Changement de code avec verrouillage	[3]/[21](Note 1)	O	1

Tableau 27/Q.765.1 – Eléments d'information transportés dans le paramètre APP *(fin)*

Elément d'information	Réf.	Type	Longueur
Changement de code sans verrouillage	[3]/[21](Note 1)	O	1
Fin de numérotation	[2]/[21](Note 1)	O	1
Compteur de transits	[6]/[21](Note 1)	O	3
NOTE 1 – La définition de ces éléments d'information par l'ISO/CEI (références [2]/[3]/[6]) et par l'UIT-T (références [21]/[22]) est identique et donc applicable dans les deux cas. NOTE 2 – Ces éléments d'information peuvent être répétés. NOTE 3 – Les éléments d'information transportés dans le paramètre de transport d'application sont pris en compte quel que soit l'ordre dans lequel ils sont reçus, à l'exception des éléments changement de code avec verrouillage et changement de code sans verrouillage, qui doivent être traités dans l'ordre spécifié.			

14.2 Informations propres à l'interface NNI, à transporter dans le paramètre de transport d'application

Les informations propres à l'interface NNI pour l'application VPN sont transportées dans le paramètre APP comme suit.

	8	7	6	5	4	3	2	1
1	Ext.	rés.	ind. CNID		SAI	GR	GT	VTI
2	Longueur du CNID							
3	CNID							
:								
14								

a) indication de transparence aux éléments VPN (VTI, *VPN feature transparency indication*)

0 pas d'indication

1 appel avec capacité de transparence aux éléments VPN;

b) capacité de transformation en nœud PINX passerelle (GT, *gateway PINX transformation capability*)

0 pas d'indication

1 PINX avec capacité de transformation en passerelle

c) indication de demande de nœud PINX passerelle (GR, *gateway PINX request indication*)

0 pas d'indication

1 demande de nœud PINX passerelle

d) indicateur d'acquittement d'établissement (SAI, *setup acknowledgement indicator*)

0 pas d'indication

1 acquittement d'établissement

e) indicateur d'identificateur de réseau de télécommunication d'entreprise (indicateur CNID)

00 indicateur non inclus (option réseau)

01 selon réseau (option réseau)

10 valeur globale

11 réserve

f) indicateur d’extension (Ext)

0 les informations continuent dans l’octet suivant

1 dernier octet

g) longueur de l'identificateur de réseau de télécommunication d'entreprise (longueur CNID)

Nombre d'octets contenant l'identificateur CNID

Lorsque l'indicateur CNID est codé 00 ("Indicateur non inclus"), la longueur du CNID est omise.

h) identificateur de réseau de télécommunication d'entreprise (CNID)

Valeur binaire

Lorsque l'indicateur CNID est codé 00 ("indicateur non inclus"), les octets 3 à 14 sont omis.

Lorsque l'indicateur de réseau de télécommunication d'entreprise choisi est la "valeur globale", l'identificateur de réseau de télécommunication contient la représentation binaire de l'identificateur de réseau de télécommunication d'entreprise. L'identificateur de réseau de télécommunication d'entreprise (CNID) commence par la représentation en BCD (décimal codé binaire) des chiffres de l'indicatif E.164 du pays où le réseau de télécommunication d'entreprise a été initialement assigné. Le reste de l'identificateur est choisi par le pays lui-même.

15 Temporisateurs

Le présent paragraphe spécifie tous les temporisateurs de processus d'application et de protocole qui correspondent aux applications VPN. Pour chaque temporisateur, on indique la valeur d'expiration, la cause ou l'armement, l'événement (les événements) de terminaison normale et les actions à exécuter à l'expiration de la temporisation. On trouvera par ailleurs, dans la dernière colonne, une référence à la description complète de la procédure concernant le processus d'application ou l'élément ASE correspondant.

15.1 Temporisateurs contenus dans l'utilisateur TC

Voir le Tableau 28.

Tableau 28/Q.765.1 – Temporisateurs contenus dans l'utilisateur TC

Symbole	Valeur d'expiration	Cause d'armement	Terminaison normale	Action à l'expiration	Référence
T1	1-5 s	Envoi de l'opération SETUP.Invoke	Réception de l'opération SETUP.ReturnResult	Abandon du dialogue Envoyer TC-U-ABORT Informer la fonction de gestion	11.4.3.1
T2	1-5 s	Envoi de l'opération ActivityTest.invoke	Réception de l'opération ActivityTest.ReturnResult	Abandon du dialogue envoyer TC-U-ABORT Informer la fonction de gestion	11.4.3.2
T3	10-60 min	Réception des opérations Setup.ReturnResult Connect.Invoke VPNFacility.Invoke ActivityTest.ReturnResult Envoi de l'opération VPNFacility.Invoke	Réception des opérations Connect.Invoke VPNFacility.Invoke Release.Invoke Envoi de l'opération ActivityTest.Invoke	Envoyer l'opération ActivityTest.Invoke	11.4.3.3
T4	10-60 min (noter que T4 doit être plus long que T3)	Réception de l'opération VPNFacility.Invoke Envoi des opérations Setup.ReturnResult Connect.Invoke VPNFacility.Invoke ActivityTest.ReturnResult	Réception de l'opération ActivityTest.Invoke Envoi des opérations Connect.Invoke VPNFacility.Invoke Release.Invoke	Abandon du dialogue Envoyer TC-U-ABORT Informer la fonction de gestion	11.4.3.4

SERIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série B	Moyens d'expression: définitions, symboles, classification
Série C	Statistiques générales des télécommunications
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	RGT et maintenance des réseaux: systèmes de transmission, de télégraphie, de télécopie, circuits téléphoniques et circuits loués internationaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	**Commutation et signalisation**
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	Réseaux pour données et communication entre systèmes ouverts
Série Y	Infrastructure mondiale de l'information
Série Z	Langages de programmation