UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T Y.140.1

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

(03/2004)

SÉRIE Y: INFRASTRUCTURE MONDIALE DE L'INFORMATION, PROTOCOLE INTERNET ET RÉSEAUX DE NOUVELLE GÉNÉRATION

Infrastructure mondiale de l'information – Généralités

Guide pour les attributs et prescriptions d'interconnexion entre opérateurs de réseaux publics de télécommunication et fournisseurs de services de télécommunication

Recommandation UIT-T Y.140.1

RECOMMANDATIONS UIT-T DE LA SÉRIE Y

INFRASTRUCTURE MONDIALE DE L'INFORMATION, PROTOCOLE INTERNET ET RÉSEAUX DE NOUVELLE GÉNÉRATION

INFRASTRUCTURE MONDIALE DE L'INFORMATION	
Généralités	**Y.100–Y.199**
Services, applications et intergiciels	Y.200–Y.299
Aspects réseau	Y.300–Y.399
Interfaces et protocoles	Y.400–Y.499
Numérotage, adressage et dénomination	Y.500–Y.599
Gestion, exploitation et maintenance	Y.600–Y.699
Sécurité	Y.700–Y.799
Performances	Y.800–Y.899
ASPECTS RELATIFS AU PROTOCOLE INTERNET	
Généralités	Y.1000–Y.1099
Services et applications	Y.1100–Y.1199
Architecture, accès, capacités de réseau et gestion des ressources	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interfonctionnement	Y.1400–Y.1499
Qualité de service et performances de réseau	Y.1500–Y.1599
Signalisation	Y.1600–Y.1699
Gestion, exploitation et maintenance	Y.1700–Y.1799
Taxation	Y.1800–Y.1899
RÉSEAUX DE LA PROCHAINE GÉNÉRATION	
Cadre général et modèles architecturaux fonctionnels	Y.2000–Y.2099
Qualité de service et performances	Y.2100–Y.2199
Aspects relatifs aux services: capacités et architecture des services	Y.2200–Y.2249
Aspects relatifs aux services: interopérabilité des services et réseaux dans les réseaux de nouvelle génération	Y.2250–Y.2299
Numérotage, nommage et adressage	Y.2300–Y.2399
Gestion de réseau	Y.2400–Y.2499
Architectures et protocoles de commande de réseau	Y.2500–Y.2599
Sécurité	Y.2700–Y.2799
Mobilité généralisée	Y.2800–Y.2899

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

Recommandation UIT-T Y.140.1

Guide pour les attributs et prescriptions d'interconnexion entre opérateurs de réseaux publics de télécommunication et fournisseurs de services de télécommunication

Résumé

Etablie sur la base du cadre général défini dans la Rec. UIT-T Y.140, la présente Recommandation porte sur l'un des scénarios d'interconnexion applicables à l'infrastructure mondiale de l'information (GII, *global information infrastructure*), à savoir l'interconnexion entre opérateurs de réseau de télécommunication public (PTNO, *public telecommunication network operator*) et fournisseurs de services. Après une analyse de la situation avant et pendant la transition vers une implémentation complète du modèle d'entreprise, la présente Recommandation contient une description détaillée des attributs des points de référence d'interconnexion entre opérateurs PTNO et fournisseurs de services. Des paragraphes distincts traitent des divers aspects de ces attributs (sécurité, interaction de services, taxation/facturation, disponibilité de service, accès à une adresse de réseau et gestion). Le contenu de la présente Recommandation est destiné à servir de guide aux parties qui implémenteront le concept d'infrastructure GII dans un réseau de prochaine génération.

Source

La Recommandation Y.140.1 de l'UIT-T a été approuvée le 29 mars 2004 par la Commission d'études 13 (2001-2004) de l'UIT-T selon la procédure définie dans la Recommandation UIT-T A.8.

Mots clés

Infrastructure mondiale de l'information, interconnexion, interfaces d'interconnexion, points de référence d'interconnexion, politique publique, prescriptions essentielles pour la fourniture de service.

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.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude 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 1 de l'AMNT.

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.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

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

Introduction

La présente Recommandation vise à compléter la Rec. UIT-T Y.140 concernant un aspect particulier. Le lecteur est supposé connaître le contenu de la Rec. UIT-T Y.140 et les considérations qui y sont présentées.

La Rec. UIT-T Y.140 décrit les points de référence d'interconnexion technique entre diverses entités intervenant dans la fourniture de services de télécommunication. Elle précise qu'une interconnexion technique est notamment requise "pour l'accès et/ou l'interconnexion d'un fournisseur de services aux produits d'un opérateur de réseau public" (§ 8 (b) de la Rec. UIT-T Y.140).

La présente Recommandation décrit en détail cette relation entre le fournisseur de services et l'opérateur de réseau ainsi que les éléments de l'interface d'interconnexion résultant de cette relation.

Il convient tout d'abord de préciser que les éléments de l'interconnexion technique entre ces deux entités – l'opérateur de réseau et le fournisseur de services – ne découlent pas uniquement des besoins de ces deux entités. Ces éléments dépendent aussi de forces externes. Par exemple, les besoins des abonnés à un service auront une influence sur la nature de l'interconnexion entre l'opérateur de réseau et le fournisseur de services. De même, des organes publics de réglementation peuvent imposer certaines exigences concernant la nature de l'interconnexion entre les deux parties. (Il est à noter au passage qu'il peut exister une relation inverse entre d'une part la mesure dans laquelle l'opérateur de réseau et le fournisseur de services tiennent compte volontairement des besoins de l'abonné à un service et d'autre part la nécessité d'une réglementation publique, dans le cadre de la politique publique, visant à obliger les deux entités à tenir compte de ces besoins. Si l'opérateur de réseau et le fournisseur de services agissent volontairement dans le sens de la politique publique, la nécessité d'une réglementation publique sera réduite. Cette relation est également appelée co-réglementation.)

Par ailleurs, la nature de l'interconnexion technique qui est convenue entre les deux parties devra faire l'objet d'un accord contractuel entre ces deux parties.

La Figure 1 illustre les relations entre les parties concernées sous la forme d'un diagramme. La présente Recommandation porte sur les aspects techniques de l'interconnexion entre l'opérateur de réseau et le fournisseur de services (la zone ombrée). Toutefois, il faut bien avoir à l'esprit que les intérêts des autres parties (identifiées dans le diagramme à l'extérieur de la zone ombrée) peuvent avoir une incidence sur cette interconnexion. Ainsi, bien que la présente Recommandation ne porte que sur la zone ombrée, elle précise, en certains endroits, l'influence que ces forces externes peuvent avoir sur les points de référence considérés. De même, les accords contractuels sortent du cadre de la présente Recommandation, mais celle-ci identifie, en certains endroits, les points de référence sur lesquels des accords contractuels externes peuvent avoir une incidence.

On trouvera davantage d'informations générales concernant l'influence que peut avoir l'environnement réglementaire changeant sur les aspects techniques de ces points de référence dans la bibliographie jointe.

Recommandation UIT-T Y.140.1

Guide pour les attributs et prescriptions d'interconnexion entre opérateurs de réseaux publics de télécommunication et fournisseurs de services de télécommunication

1 Domaine d'application et objet

La présente Recommandation porte sur l'interconnexion entre un fournisseur de services et un réseau (public) (ce type d'interconnexion sera plus simplement appelé accès d'un fournisseur de services). Les parties concernées ne doivent pas considérer la présente Recommandation comme une obligation mais comme un guide destiné à les aider à identifier et à mettre en œuvre volontairement les attributs/prescriptions essentiels appropriés permettant de satisfaire aux objectifs de la politique publique.

Il convient donc d'examiner deux aspects/perspectives:

a) les prescriptions des fournisseurs de services vis-à-vis des opérateurs de réseau pour la fourniture de services de télécommunication;

b) les prescriptions des opérateurs de réseau concernant l'offre d'un accès aux fournisseurs de services.

La Rec. UIT-T Y.140 définit un ensemble possible de points de référence d'interconnexion (RPI, *reference point for interconnection*), illustré sur la Figure 1/Y.140. Au § 8/Y.140, il est précisé que des attributs/prescriptions essentiels sont nécessaires concernant les différentes classes d'interface d'interconnexion. La classe b concerne l'interconnexion entre fournisseurs de services et (produits d') opérateurs de réseau public. La présente Recommandation propose une description des attributs/prescriptions pour les interfaces d'interconnexion de la classe b.

L'accès indirect d'un fournisseur de services, autrement dit un accès pour lequel il existe des réseaux intermédiaires, ne sera pas considéré dans la présente Recommandation.

Un exemple de scénario possible est donné sur la Figure 1. Celle-ci représente un environnement avec de nombreuses parties différentes et les relations qui existent entre ces parties. La présente Recommandation ne porte que sur la zone ombrée.

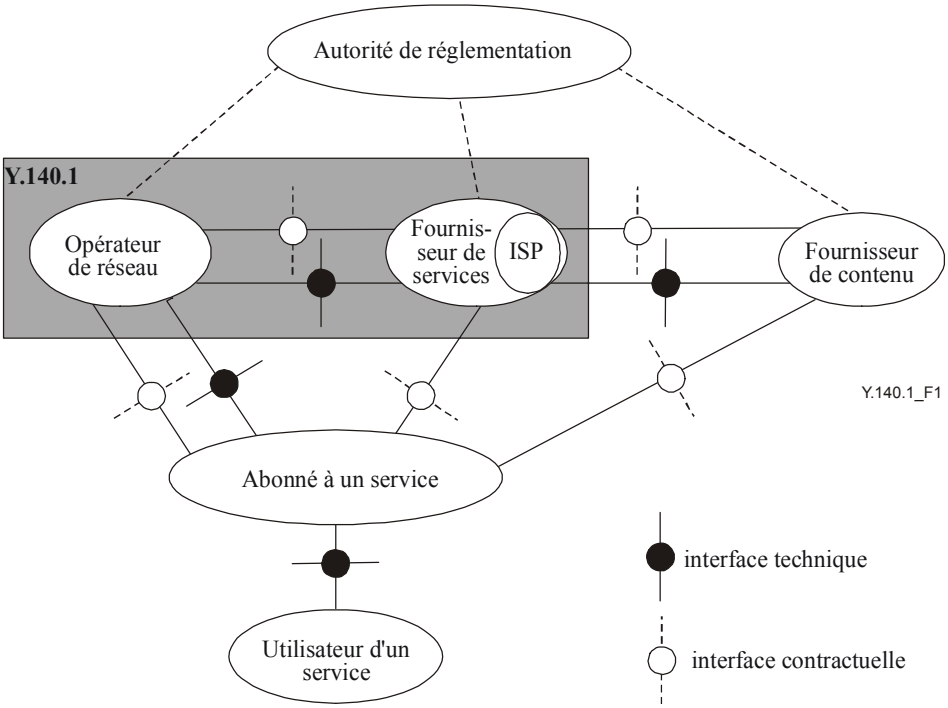

Figure 1/Y.140.1 – Exemple de relations entre les parties concernées

La présente Recommandation décrit les prescriptions fonctionnelles génériques concernant l'accès d'un fournisseur de services. Le niveau de priorité de chaque prescription est fondé sur le degré de nécessité perçu par le fournisseur de services a) ou par l'opérateur de réseau (public) b). Pour satisfaire à ces prescriptions, il faudra améliorer les protocoles existants ou en élaborer de nouveaux en tenant dûment compte des considérations relatives à l'intégrité des réseaux.

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. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

[1] Recommandation UIT-T F.115 (1995), *Objectifs de service et principes relatifs aux futurs systèmes mobiles terrestres publics de télécommunication*.

[2] Recommandation UIT-T H.235 (2003), *Sécurité et chiffrement pour les terminaux multimédias de la série H (terminaux H.323 et autres terminaux de type H.245)*.

[3] Recommandation UIT-T J.93 (1998), *Prescriptions d'accès conditionnel dans le réseau de distribution secondaire de la télévision numérique par câble*.

[4] Recommandation UIT-T J.95 (1999), *Protection antipiratage de la propriété intellectuelle des émissions diffusées sur les systèmes de télévision par câble*.

[5] Recommandation UIT-T Q.1290 (1998), *Glossaire utilisé dans la définition des réseaux intelligents*.

[6] Recommandation UIT-T X.800 (1991) | ISO/CEI 7498-2:1989, *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT*.

[7] Recommandation UIT-T Y.140 (2000), *Infrastructure mondiale de l'information: cadre général des points de référence d'interconnexion*.

[8] ISO/CEI 7498-2:1989, *Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Modèle de référence de base – Partie 2: Architecture de sécurité*.

[9] ETSI ES 201671 V2.1.1 (2001), *Telecommunications security; Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic*.

[10] ETSI TS 101 331 V1.1.1 (2001), *Telecommunications security; Lawful Interception (LI); Requirements of Law Enforcement Agencies*.

[11] ETSI ETR 232 ed.1 (1995), *Glossary of security terminology*.

[12] ETSI EG 201 722 V1.2.1 (2000), *Intelligent Network (IN); Service provider access requirements; Enhanced telephony services*.

[13] ETSI EG 201 781 V1.1.1 (2000), *Intelligent Network (IN); Lawful interception*.

[14] ETSI EG 201 807 V1.1.1 (2000), *Network operators' requirements for the delivery of service provider access*.

[15] ETSI EG 201 897 V1.2.1 (2002), *Service Provider Access Requirements in a Fixed and Mobile Environment*.

[16] ETSI EG 201 899 V1.1.1 (2001), *Modelling Service Provider Access Requirements using an API Approach*.

[17] ETSI EG 201 916 V1.1.1 (2001), *Development of standards to support Open Inter-Network Interfaces and Service Provider Access*.

[18] ETSI EG 201 965 V1.1.1 (2001), *Service Provider Access Management Requirements for Open Network Access*.

3 Termes et définitions

Dans la présente Recommandation, le terme "service" est utilisé dans un sens large, il ne s'agit pas strictement d'un "service de télécommunication" tel que ce terme est défini par la CE 2 de l'UIT-T.

Dans la présente Recommandation, les définitions suivantes s'appliquent:

3.1 authentification: processus permettant de vérifier avec certitude l'identité d'une entité participant à une communication. L'authentification, qui suit généralement l'identification, permet d'établir la validité de l'identité déclarée et d'empêcher toute action frauduleuse.

3.2 disponibilité[1]: propriété d'être accessible et utilisable sur demande par une entité autorisée [8], [6].

3.3 confidentialité[1]: propriété d'une information qui n'est ni disponible, ni divulguée aux personnes, entités ou processus non autorisés [8], [5].

3.4 (Protection contre les) fraudes

3.4.1 fraude: fait d'obtenir un avantage financier par le biais d'une fausse représentation ou d'une action non autorisée.

3.4.2 fraudeur: entité commettant une fraude.

---

[1] Les définitions des termes sécurité, disponibilité, intégrité et confidentialité sont étroitement liées et doivent être utilisées dans le contexte les unes des autres.

3.4.3 fraude d'équipement: utilisation frauduleuse du réseau de télécommunication faisant intervenir une utilisation abusive d'un équipement terminal, par exemple d'un téléphone public.

3.4.4 fraude de réseau: utilisation frauduleuse de l'infrastructure du réseau de télécommunication faisant intervenir une utilisation abusive d'installations techniques du réseau, parfois à partir d'un équipement terminal.

3.4.5 fraude de service: utilisation frauduleuse de services de télécommunication, faisant parfois intervenir l'interaction attendue ou inattendue de deux services ou plus.

3.4.6 fraude d'abonnement: utilisation frauduleuse du réseau de télécommunication par une entité qui n'a pas l'intention de régler la facture qu'elle doit payer.

3.4.7 fraude de télécommunication: fraude qui est commise directement à l'encontre du réseau de télécommunication ou de ses abonnés.

3.5 Intégrité[1]

a) Propriété de données qui n'ont été ni altérées ni détruites de manière non autorisée [8], [6], [5].

b) Capacité d'une fonction à résister aux usurpations en vue d'utilisations non autorisées et aux modifications en vue de donner des résultats non autorisés [3], [4].

3.6 interception licite: action (fondée sur la législation) exécutée par un opérateur de réseau/un fournisseur d'accès/un fournisseur de services et consistant à rendre certaines informations disponibles et à les fournir à un organisme chargé de surveiller l'application de la loi [13].

3.7 secret:

– secret des communications: mode de communication dans lequel seules les entités explicitement habilitées peuvent interpréter la communication. Le secret des communications est normalement réalisé par chiffrement et par partage de clé(s) pour accéder au chiffre [2];

– respect de la vie privée: droit des individus de contrôler ou d'agir sur des informations les concernant, qui peuvent être collectées et stockées, et sur les personnes par lesquelles et auxquelles ces informations peuvent être divulguées.

NOTE – Ce terme étant lié au droit privé, il ne peut pas être très précis et son utilisation devrait être évitée sauf pour des besoins de sécurité [6], [1].

3.8 politique publique: dans le contexte des télécommunications, une politique publique est une politique qui est établie par les organes de réglementation afin de répondre à l'intérêt public, politique qu'ils peuvent mettre en application par le biais de réglementations imposées aux entités de télécommunication.

3.9 sécurité[1]: protection de la disponibilité, de l'intégrité et de la confidentialité des informations [11].

4 Abréviations

La présente Recommandation utilise les abréviations suivantes:

NNI interface réseau-réseau (*network-network interface*)

PTN réseau téléphonique public (*public telecommunication network*)

PTNO opérateur de réseau téléphonique public (*public telecommunication network operator*)

---

[1] Les définitions des termes sécurité, disponibilité, intégrité et confidentialité sont étroitement liées et doivent être utilisées dans le contexte les unes des autres.

SLA accord sur le niveau de service (*service level agreement*)

SP fournisseur de services (*service provider*)

SPA accès d'un fournisseur de services (*service provider access*)

SPAI interface d'accès d'un fournisseur de services (*service provider access interface*)

SPAR prescription(s) d'accès d'un fournisseur de services (*service provider access requirement(s)*)

NOTE – Le terme Service (avec un S majuscule) est évité car c'est un terme "réservé" à l'usage de la CE 2.

5 Sécurité

Dans la présente Recommandation, les problèmes liés à la sécurité sont examinés au paragraphe 7 "Attributs des points de référence d'interconnexion entre opérateurs PTNO et fournisseurs de services", et en particulier au § 7.1 "Sécurité". Ce paragraphe traite des aspects de sécurité par rapport au point de vue des utilisateurs finals d'une part et des fournisseurs de services et opérateurs PTNO d'autre part. Il traite en outre des aspects d'intégrité (§ 7.1.1), d'authentification (§ 7.1.2) et de confidentialité (§ 7.1.3), concepts qui sont étroitement liés à la sécurité. Comme la présente Recommandation est destinée avant tout à servir de guide, elle aborde essentiellement des aspects de sécurité de caractère général. A cet égard, la plupart des documents de l'ETSI énumérés au paragraphe 2 "Références (informatives)" sont des guides.

6 Situation avant et pendant la transition vers une implémentation complète du modèle d'entreprise

Actuellement, le modèle d'entreprise décrit dans la Rec. UIT-T Y.110 n'est pas complètement implémenté. Dans le passé, les réseaux étaient essentiellement conçus pour les services que les opérateurs de réseau proprement dits souhaitaient offrir à leurs clients. Cela étant, il suffisait, dans la plupart des cas, de concevoir les réseaux de manière telle que les opérateurs de réseau puissent produire et délivrer leurs "propres" services. Il suffisait donc de prévoir un appui technique uniquement en interne en ce qui concerne l'accès, la facturation, la signalisation, l'intégrité, la gestion, etc. Même si ces services étaient fournis par l'intermédiaire de plusieurs réseaux (par exemple par l'intermédiaire de plusieurs pays ou d'opérateurs de réseau concurrentiels), il n'était pas vraiment nécessaire de prendre en charge l'accès de tiers aux fonctions internes de réseau. Compte tenu de la prise de décisions politiques visant à faire confiance aux forces du marché et à ouvrir le marché, des modifications fondamentales de l'environnement de réglementation des télécommunications se sont produites.

Pour stimuler la concurrence, les organes de réglementation ont d'abord obligé les opérateurs de réseau existants à permettre l'accès de tiers à tout ou partie de leurs réseaux.

Avec l'accentuation de la libéralisation et la mise en place de nouvelles technologies, la conception des réseaux de télécommunication a changé. Les changements importants en termes de philosophie et d'architecture sont par exemple décrits dans les Recommandations UIT-T Y.110 et Y.140.

Cette "nouvelle approche" se traduit par des modifications fondamentales du secteur des télécommunications en termes de propriété, de structure de marché et de progrès techniques, qui engendrent bon nombre de problèmes. Pour faire face à cette nouvelle situation, il faut concilier les intérêts différents et parfois divergents d'au moins trois parties (l'utilisateur final, l'opérateur de réseau et le fournisseur de services tiers).

L'une des nécessités les plus importantes est de garantir l'intégrité du réseau, des services et des données. Alors que dans le passé, l'ensemble de la gestion y compris la production de services relevait d'une seule partie (l'opérateur de réseau), il faut maintenant ouvrir au moins certaines parties de la gestion de réseau pour pouvoir assurer notamment la signalisation, la réservation de

largeur de bande, la facturation et la taxation nécessaires à la fourniture de services. Un fournisseur de services peut souhaiter obtenir un accès plus ou moins direct au réseau. En l'absence de mesures additionnelles, cet accès risque d'entraîner une perte d'intégrité et/ou de confidentialité des autres services et/ou des données des autres utilisateurs acheminés sur le réseau (de transport) initial. De plus, cet accès risque d'empêcher à l'opérateur du réseau initial d'offrir un plan de priorité pour les télécommunications d'urgence.

Un fournisseur de services peut également souhaiter avoir accès à des informations concernant les capacités des terminaux afin d'offrir un service personnalisé ou de "modifier" les capacités, le comportement, les fonctionnalités et les conditions d'un terminal. Si l'accord explicite et individuel de l'utilisateur n'est pas demandé, les droits de l'utilisateur et éventuellement ceux d'autres parties seraient alors bafoués. Il faut donc mettre en place, dans les terminaux, dans les réseaux de transport et dans la fourniture de services, des mécanismes qui permettent de tenir compte et de respecter les intérêts et les droits des parties concernées.

Ces scénarios peuvent servir d'exemple pour les prescriptions/attributs qui peuvent être nécessaires afin de mettre en œuvre le modèle d'entreprise décrit dans la Rec. UIT-T Y.110 et de répondre aux besoins d'un marché des télécommunications entièrement concurrentiel.

La présente Recommandation examine plusieurs propriétés/attributs (la liste n'est pas exhaustive) des points de référence d'interconnexion (RPI), qui devraient faciliter l'élaboration d'interfaces visant à respecter, dans la mesure du possible, les intérêts des parties concernées.

7 Attributs des points de référence d'interconnexion entre opérateurs PTNO et fournisseurs de services

NOTE – Le contenu de ce paragraphe est fondé sur les Guides de l'ETSI [12] à [18].

Les relations mutuelles entre un opérateur PTNO et un fournisseur de services font généralement l'objet d'accords sur le niveau de service (SLA, *service level agreement*). Ces accords précisent les informations que le fournisseur de services et l'opérateur PTNO doivent échanger et les mécanismes qu'ils doivent utiliser à cette fin.

7.1 Sécurité

NOTE – Le site Web de l'UIT contient des informations régulièrement mises à jour sur les questions relatives à la sécurité [B-7].

Les utilisateurs finals, les fournisseurs de services et les opérateurs PTNO ont chacun des objectifs et des besoins différents en ce qui concerne la fourniture de services de télécommunication sur les réseaux de télécommunication publics. Un certain nombre de ces objectifs ont été identifiés. Pour qu'ils puissent être satisfaits, les aspects de sécurité doivent être dûment pris en compte dans un nouvel environnement comportant une multitude d'interconnexions et de configurations d'accès relatives aux fournisseurs de services.

Il est possible que les besoins des utilisateurs finals et ceux des autres parties intervenant dans la fourniture de services ne soient pas tous compatibles. Un utilisateur peut par exemple souhaiter visiter des sites web de façon anonyme, tandis que des autorités de poursuites judiciaires peuvent souhaiter suivre certaines activités de navigation sur le Web.

Les risques de sécurité généraux sont notamment les suivants: mystification anti-utilisateur (usurpation d'identité illicite, attaques de type reprise d'identité, détournement et vol de service, etc.); perte d'intégrité des données (les données doivent correspondre exactement aux données qui ont été envoyées: pas d'ajout, pas de modification, pas de suppression), écoute clandestine (écoute, copie de données), perte de confidentialité des données/du service (les parties en communication doivent avoir la garantie que leur communication est bien privée), absence de fiabilité des parties utilisées pour accéder à des données/faire transiter des données, répudiation (le destinataire de

données doit obtenir la preuve irréfutable que les données ont été envoyées, conservées et générées par une source fiable) et les attaques de déni de service.

Les sommes de contrôle, l'authentification et le chiffrement permettent de résoudre certains de ces problèmes; quant à la non-répudiation et à la protection contre les attaques de déni de service, il n'existe pas de solution immédiate fondée sur les services. Les réseaux et les protocoles doivent être conçus de manière à faire face à ces problèmes au moins partiellement. D'autres aspects de la fraude concernent le non-respect de certaines règles (par exemple le refus de payer, le vol, etc.). Les réseaux nécessiteront la mise en place d'une comptabilité et d'une traçabilité sécurisées et fiables afin d'être protégés contre le vol de service et le détournement de l'utilisation de ressources.

Du point de vue des utilisateurs finals, les prescriptions essentielles sont les suivantes:

– disponibilité des services;
– facturation correcte;
– protection contre les fraudes;
– confidentialité;
– anonymat [parfois];
– respect de la vie privée.

Du point de vue des fournisseurs de services et des opérateurs PTNO, les prescriptions essentielles sont les suivantes:

– disponibilité du réseau, des services et de la maintenance;
– taxation correcte;
– capacité de garder une trace des appels individuels;
– protection des données relatives aux abonnés contre le piratage;
– élimination de l'utilisation frauduleuse de leurs équipements.

Les violations de sécurité peuvent avoir d'importantes conséquences financières négatives à la fois pour les fournisseurs de services et pour les opérateurs de réseau (perte de recettes, perte de réputation, perte de part de marché par exemple).

En particulier, l'intégrité de réseau est une question essentielle lorsque des relations inter-réseaux sont établies entre opérateurs PTNO et fournisseurs de services.

En ce qui concerne l'accès d'un fournisseur de services (accès SPA), un ensemble de fonctionnalités de base peut être nécessaire pour sécuriser l'interface entre l'opérateur PTNO et le fournisseur de services. Une analyse des menaces concernant les interconnexions fondées sur le réseau intelligent est présentée dans le document ETSI TR 101 365 et des lignes directrices relatives aux mesures de sécurité applicables sont données dans le document ETSI TR 101 664.

Des fonctions de filtrage et de mappage sont utilisées pour contrôler et sécuriser les accords bilatéraux sur les interfaces entre les réseaux PTN. Actuellement, les opérateurs PTNO disposent de fonctionnalités de filtrage et de mappage sur certaines des interfaces NNI d'interconnexion (par exemple les connexions du sous-système utilisateur du RNIS du système de signalisation n° 7). Ces fonctionnalités et fonctions doivent être étendues progressivement afin que toutes les interfaces entre les opérateurs PTNO et les fournisseurs de services en soient dotées.

D'autres aspects de sécurité associés aux réseaux mobiles, à l'Internet et aux réseaux large bande concernent le transfert d'informations d'identité de terminal/d'identité personnelle (par exemple identité internationale d'abonné mobile IMSI, signature électronique, etc.) entre l'environnement de l'utilisateur et le fournisseur de services ou la prise en charge d'une transmission de bout en bout sécurisée entre le terminal d'utilisateur et l'application du fournisseur de services (protocole SSL, *secure socket layer*), techniques de chiffrement, etc.).

7.1.1 Intégrité

NOTE – Pour plus d'informations sur les responsabilités en matière de garantie du maintien de l'intégrité des réseaux dans un environnement interconnecté, on se reportera au document [B-6].

L'intégrité de réseau, qui relève de la gestion de réseau, est la capacité du réseau à conserver certaines caractéristiques de qualité de fonctionnement et de fiabilité.

L'intégrité de réseau est une question essentielle lorsqu'une relation de réseau est établie entre un réseau PTN et un fournisseur de services. Lorsqu'un réseau PTN est ouvert à un fournisseur de services, l'accès aux données/informations stockées est élargi. Les données doivent être protégées convenablement par l'utilisation de mots de passe et par le recours au partitionnement, de sorte que l'intégrité et le respect de la vie privée ne soient pas compromis.

L'intégrité de réseau sous-entend aussi la garantie de l'intégrité des éléments de réseau et la fourniture d'un niveau de service acceptable. Les vulnérabilités associées à l'intégrité des systèmes peuvent entraîner une interruption ou un déni de service, ou la modification non autorisée d'informations d'utilisateur ou de réseau et de services de réseau.

Pour pouvoir prendre en charge les services améliorés des fournisseurs de services, une évolution des réseaux PTN est nécessaire et, pour cela, il faut planifier la croissance de la capacité de commutation en temps réel en tenant compte de l'émergence de ce nouveau service d'accès. Les opérateurs PTNO et les fournisseurs de services devraient donc négocier les aspects liés à l'ingénierie du trafic pour faire en sorte qu'une capacité de réseau adéquate soit disponible. Si les opérateurs PTNO et les fournisseurs de services ne prévoient pas convenablement l'augmentation de capacité, le réseau public sera vulnérable aux problèmes d'interruption et de déni de service.

Il convient de prendre en considération les aspects suivants:

– Une fonction passerelle entre le réseau PTN et le fournisseur de services, notamment pour les messages de taxation/facturation et leurs paramètres.
– Le mécanisme de protection visant à garantir que les fournisseurs de services n'entravent pas les services offerts dans le réseau PTN.
– Les mécanismes d'authentification/de chiffrement visant à protéger le réseau PTN contre les vulnérabilités dues à l'accès SPA.
– Par ailleurs, le maintien de l'intégrité de réseau repose sur les prescriptions suivantes:
    - des mesures de compatibilité doivent garantir que les réseaux et les fournisseurs de services avec des niveaux de qualité différents fonctionnent ensemble correctement;
    - des mécanismes permettant la prise en charge de procédures d'essais de conformité doivent exister afin de pouvoir vérifier l'interopérabilité entre un réseau PTN et un fournisseur de services;
    - l'accès SPA augmente le risque de vulnérabilités associées aux problèmes d'interaction d'éléments de service si on ne dispose pas de connaissances suffisantes pour traiter ces problèmes. L'interaction d'éléments de service peut conduire à l'interruption d'un service nécessaire ou peut permettre à des pirates informatiques de commettre des abus volontaires. Il convient d'implémenter des mesures appropriées pour éviter ce type de risque.

Compte tenu de la plage de services offerts par les fournisseurs de services, l'accès SPA reposera probablement sur différents types d'interface, qui nécessiteront peut-être des ensembles de fonctionnalités différents au niveau de la passerelle à la frontière du réseau.

Dans les futures implémentations, il conviendra tout particulièrement de tenir compte des points de vue des opérateurs PTNO, des fournisseurs de services et des utilisateurs/abonnés/clients.

7.1.2 Authentification

Dans le cadre de "qui doit s'authentifier auprès de qui", plusieurs sous-aspects sont à considérer:

– un utilisateur auprès d'un fournisseur de services et/ou d'un opérateur PTNO (par exemple en cas d'accès);

– un fournisseur de services auprès d'un opérateur PTNO;

– un opérateur PTNO auprès d'un autre (par exemple lorsque des réseaux par paquets interviennent ou lorsque des connexions virtuelles comprenant une tunnellisation interviennent);

– un fournisseur de services auprès d'un autre s'ils utilisent différents niveaux ("semi-produits") de la chaîne de valeurs ajoutées.

Il existe par ailleurs un type "d'authentification implicite" fondée sur des droits de priorité (par exemple en cas de communications d'urgence). En général, il faut faire une distinction entre le processus de vérification proprement dit et le mécanisme implicite, c'est-à-dire entre qui vérifie et comment faire comprendre le résultat aux partenaires de la "chaîne d'authentification".

Pour l'authentification, on utilise généralement des numéros PIN, des cartes SIM ou des signatures numériques (par exemple dans le contexte des communications mobiles).

Dans les futures implémentations, il conviendra tout particulièrement de tenir compte des points de vue des opérateurs PTNO, des fournisseurs de services et des utilisateurs/abonnés/clients.

7.1.3 Confidentialité

La confidentialité est une prescription essentielle pour les affaires. Il est relativement simple de maintenir la confidentialité en cas de réunions en tête à tête où seuls les partenaires directement concernés sont présents. Mais cela devient plus difficile en cas de télécommunication publique via des tiers tels que des opérateurs PTNO et des fournisseurs de services (ou des installations de tiers). On peut distinguer plusieurs niveaux de maintien de la confidentialité, par exemple les niveaux suivants, par ordre croissant de difficulté de garantie de la confidentialité:

Niveau 1: les contrats sont échangés par courrier postal ou par fax. Le "secret des courriers" dans le premier cas et le "secret des télécommunications" dans le second cas garantissent un certain degré de confidentialité.

Niveau 2: les contrats sont échangés par le biais d'Internet (par exemple par courrier électronique).

Niveau 3: les contrats sont négociés par le biais de réseaux de communication.

Lorsque des réseaux de télécommunication interviennent, il faut faire une distinction entre réseau public et réseau d'entreprise (groupe fermé d'utilisateurs).

Un domaine particulièrement important dans lequel la confidentialité joue un rôle primordial est le commerce électronique.

Les signatures numériques constituent un moyen bien connu employé pour garantir la confidentialité.

7.1.3.1 Point de vue de l'opérateur de réseau de télécommunication public

Un opérateur PTNO peut contribuer au maintien de la confidentialité en veillant à ce que seules les personnes autorisées puissent intercepter des communications (voir interception licite).

7.1.3.2 Point de vue du fournisseur de services

Un domaine typique, voire le domaine le plus important, dans lequel le fournisseur de services joue un rôle en matière de confidentialité est le commerce électronique.

7.1.3.3 Point de vue de l'utilisateur/de l'abonné/du client

L'utilisateur/l'abonné/le client recherche la confidentialité absolue.

Plus le degré de confidentialité qui lui est offert est élevé, plus le prix qu'il est prêt à payer pour cette confidentialité est élevé.

7.1.4 Protection contre les fraudes

La protection contre les fraudes est un aspect essentiel du commerce électronique car:

i) l'enjeu est considérable,

ii) il existe de nombreuses possibilités d'attaque.

7.1.4.1 Point de vue de l'opérateur de réseau de télécommunication public

Un opérateur PTNO cherche à recevoir une rémunération adéquate si "ses" installations de réseau sont utilisées par quelqu'un. Les fraudes peuvent provenir d'utilisateurs/d'abonnés/de clients, de fournisseurs de services ainsi que d'autres opérateurs PTNO participant à l'ensemble du processus de communication.

7.1.4.2 Point de vue du fournisseur de services

Un fournisseur de services souhaite que les services qu'il offre ne puissent être utilisés que par les personnes autorisées, c'est-à-dire par ceux qui ont établi un contrat avec lui.

Un fournisseur de services cherche en réalité à être rémunéré pour chaque service utilisé qu'il offre contre paiement.

7.1.4.3 Point de vue de l'utilisateur/de l'abonné/du client

Un utilisateur/un abonné/un client souhaite que soient évitées les situations dans lesquelles quelqu'un d'autre utilise un service à ses frais, par exemple en utilisant son identification (numéro PIN).

7.1.5 Interception licite

L'interception licite ne concerne pas l'UIT dans la mesure où aucune autorité intergouvernementale ne lui donne mandat en la matière au niveau du système des Nations Unies (Charte de l'UIT).

Toutefois, les points de référence d'interconnexion et leurs interfaces correspondantes (voir Rec. UIT-T Y.140) devraient être conçus de manière à tenir compte des prescriptions nationales relatives à l'interception licite et ne devraient pas empêcher (exclure) l'implémentation des éventuelles mesures nationales existantes.

Pour des raisons économiques, les **fournisseurs de services** et les **opérateurs PTNO** ne souhaitent pas se voir imposer des efforts inutiles en la matière.

Les **utilisateurs** ne souhaitent pas que les mesures nécessaires à la mise en œuvre de l'interception licite ne les affectent trop.

On trouvera des indications sur les prescriptions relatives à l'interception licite et sur les solutions possibles en matière d'interception licite dans les publications [10] et [9] de l'ETSI.

7.2 Interaction de services

Dans un environnement dans lequel un utilisateur final s'abonne à un ensemble de services offerts par plusieurs fournisseurs, des interactions négatives peuvent se produire entre services et éléments de service. Il faut donc prévoir une fonctionnalité supplémentaire qui permette de gérer les interactions et ce, afin que les services puissent être fournis de manière intégrée et cohérente.

Un complément d'étude est nécessaire en ce qui concerne les interactions de service, y compris les interactions négatives qui peuvent se produire entre les équipements des opérateurs PTNO et ceux

des fournisseurs de services, lorsque plusieurs des parties intervenant dans le traitement d'appel exigent de pouvoir contrôler l'appel.

Des problèmes d'interaction de services se posent par exemple dans le cas de la combinaison des prescriptions relatives à la portabilité des numéros et des prescriptions relatives à l'accès d'un fournisseur de services. Par exemple, plusieurs prescriptions stipulent qu'une action relative à un appel peut être déclenchée par un certain fournisseur de services si l'identification de la ligne de l'appelant se trouve dans une plage de numérotation particulière. En raison des mécanismes de portabilité de service, la détection de cette plage de numérotation ne garantit pas que l'appel devra être traité par le fournisseur de services auquel la plage de numérotation a été attribuée au départ.

7.3 Taxation/facturation

Les mécanismes de taxation standards permettent de taxer un appel efficace, par exemple entre le moment où l'appelé répond et le moment où l'appel est libéré. Certaines prescriptions de fournisseurs de services impliquent une utilisation du réseau PTN qui sort de ce cas standard et il faut donc implémenter un mécanisme de taxation associé entre l'opérateur PTNO et le fournisseur de services afin de tenir compte de cette utilisation. C'est par exemple le cas pour les prescriptions suivantes des fournisseurs de services:

– demande d'ouverture d'un trajet de messages dans la bande vers l'arrière jusqu'à l'appelant initial immédiatement après l'arrivée d'une confirmation d'établissement d'appel, sans qu'un signal "de réponse" ne soit retourné;
– acheminement d'une indication d'appel inefficace depuis le réseau PTN de destination, c'est-à-dire lorsqu'une indication autre que "sonnerie" est retournée à l'appelant ou lorsqu'une situation de "non-réponse" se produit;
– fourniture d'informations relatives à la destination et au routage de l'appel afin de contrôler la destination et le routage de l'appel;
– interaction avec l'utilisateur de service avant que toute taxation du service ne commence;
– envoi de données au réseau PTN de l'utilisateur de service et réception de données en provenance de ce réseau sans signal d'alerte (sonnerie par exemple);
– les aspects de taxation et de facturation des appels, tels qu'ils sont vus par les opérateurs PTNO, sont examinés dans le document ETSI EG 201 807.

Lorsque la taxation de l'utilisateur final ne repose pas sur les mécanismes de taxation d'appel standards (par exemple si la taxation est suspendue, retardée ou modifiée), il faut créer des événements appropriés en vue d'une éventuelle journalisation afin de fournir les données nécessaires à une comptabilité appropriée entre le fournisseur de services et l'opérateur PTNO.

A titre d'exemple, le marché est demandeur:

– de facturations fondées sur l'abonnement pour l'accès Internet;
– d'abonnements prépayés avec minutes incluses pour le service fixe et le service mobile;
– de paiements à l'utilisation sans abonnement.

Tous ces cas nécessitent une comptabilité en temps réel (facturation instantanée) sur une interface de données sécurisée.

Il faut tenir compte des législations et réglementations nationales ou européennes, selon le cas, lorsque des mécanismes de taxation sont conçus et implémenté, par exemple pour la fourniture d'un avis de taxation à un utilisateur de service.

7.3.1 Point de vue de l'opérateur de réseau de télécommunication public

– Outils de signalisation pour la facturation et la taxation (en temps réel), signaux d'information de trafic évolués.

– Transmission d'informations de taxation (en temps réel) sur les réseaux.

– Les opérateurs de réseau et les fournisseurs de services ont besoin de pouvoir retrouver les informations de facturation en temps réel et exigent la non-répudiation du fait que la facture a été reçue, qu'elle était correcte, les données étant exactes et n'ayant pas été altérées.

– Il faut accorder une attention particulière à la précision de l'horloge de réseau et à l'exactitude de sa transmission, en particulier si plusieurs réseaux PTN interviennent.

7.3.2 Point de vue du fournisseur de services

– Production et soumission d'informations de taxation (en temps réel) pour le client.

7.3.3 Point de vue de l'utilisateur

– Réception d'information de taxation/facturation (en temps réel).

– Les utilisateurs/abonnés exigent une traçabilité en ce qui concerne les éléments qui leur sont facturés et l'indication du fait que le service a bien été utilisé au moment déclaré (les tickets de service, l'avis de taxation et la facturation détaillée sont des solutions possibles).

– Des aspects particulièrement importants pour l'utilisateur sont l'exactitude de la facture et une "quantification" raisonnable des intervalles sur lesquels la facturation est fondée (plus ils sont étroits, mieux c'est).

7.4 Disponibilité de service

La disponibilité de service est une question de politique entre l'utilisateur et le fournisseur de services et entre le fournisseur de services et l'opérateur de réseau et dépend de l'accord d'offre de service conclu.

Pour la disponibilité de service, on se fonde sur un "plan de priorité".

7.5 Accès à une adresse de réseau

NOTE – Bien que ce ne soit pas illustré sur la Figure 1, les relations entre les différentes parties reposent sur des aspects de nommage et d'adressage. Ces aspects peuvent relever ou non de la juridiction d'une autorité de réglementation.

Parmi les applications pour lesquelles un fournisseur de services peut avoir besoin d'accéder à une adresse de réseau, on peut citer les services d'annuaire, les demandes de renseignements en ligne, les services de renvoi, etc.

L'accès aux réseaux, aux services de réseau et aux applications nécessite que des numéros et des plages de numérotation adéquats soient prévus pour tous les services de communication électroniques disponibles publiquement et qu'ils puissent être attribués de manière objective, transparente et non discriminatoire.

7.6 Gestion

La Figure 2 illustre une architecture de référence dans laquelle sont représentés les points RPI entre un fournisseur de services et un opérateur PTNO. Cette architecture peut servir à déterminer les prescriptions des deux parties en ce qui concerne l'échange d'informations de gestion via les interfaces correspondant aux points RPI.

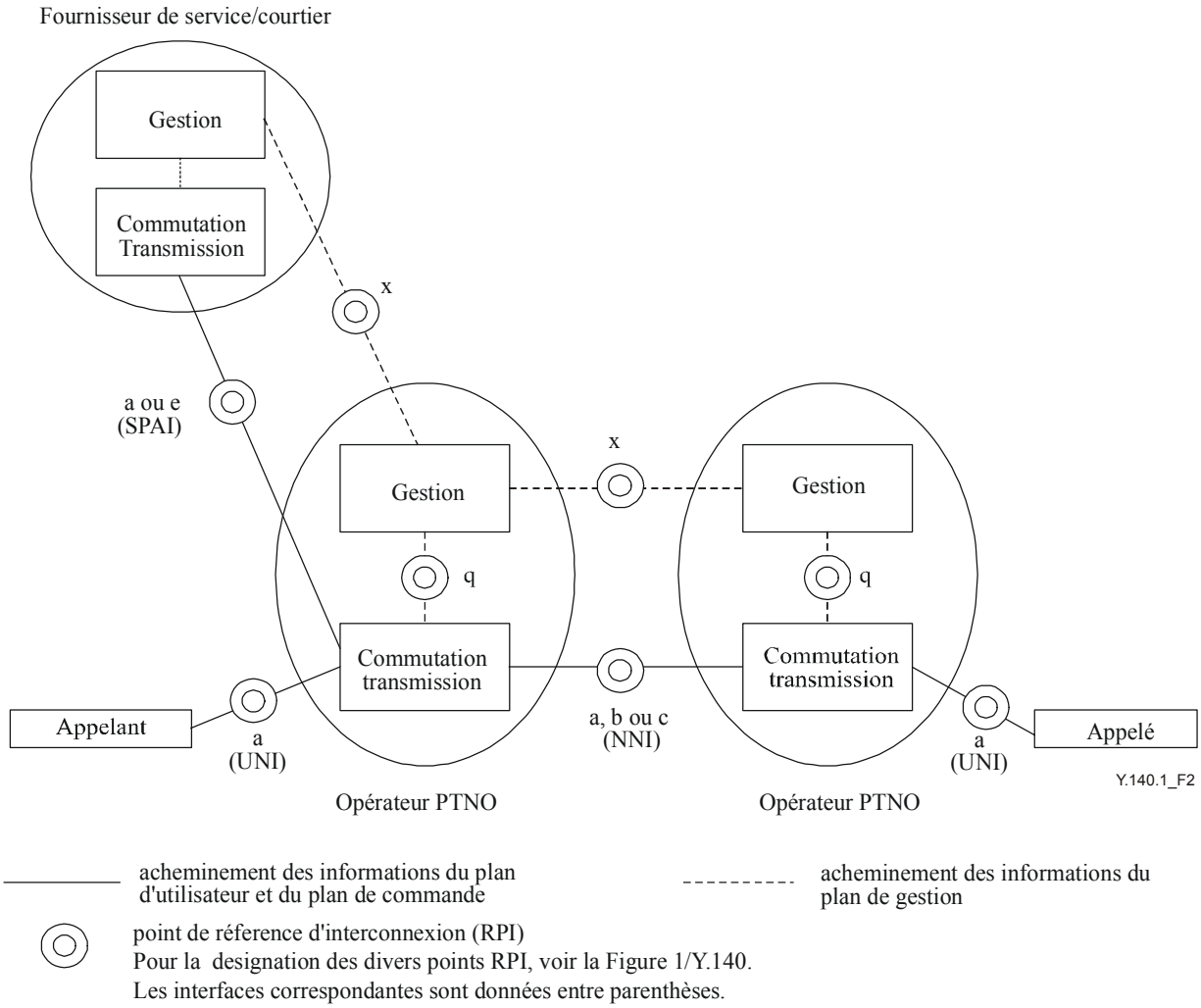

Figure 2/Y.140.1 – Architecture de référence pour les prescriptions de gestion entre un fournisseur de services et un opérateur PTNO

On trouvera une analyse détaillée de la situation dans le document [18], qui porte sur l'interface du plan de gestion entre les équipements d'un fournisseur de services et les équipements d'un opérateur de réseau téléphonique public (PTNO). Chaque prescription est fondée sur des études réalisées au sujet des prescriptions d'accès d'un fournisseur de services (SPAR) et publiées dans les documents [12] à [15]. Le document [18] précise quelles sont les prescriptions SPAR qui se rapportent à la gestion. Pour satisfaire à ces prescriptions de gestion, des protocoles appropriés seront nécessaires, sur la base des flux d'information décrits dans le document [18]. Lorsque des protocoles appropriés ne sont pas disponibles, il faudra améliorer les protocoles existants ou en élaborer de nouveaux.

Les prescriptions de gestion indiquées dans le document [18] peuvent être subdivisées en plusieurs catégories:

– capacités liées au trafic (par exemple établissement de déclencheurs de commutation, remplissage de données, etc.), nécessaires pour satisfaire à une ou plusieurs prescriptions SPAR du point de vue opérationnel;
– capacités de gestion de la performance (par exemple surveillance de la performance des liaisons entre un fournisseur de services et un réseau PTN, reconfiguration de liaison, etc.);
– liaisons électroniques/demandes de service.

8 Niveau de priorité des prescriptions aux points de référence d'interconnexion

Tableau 1/Y.140.1 – Niveau de priorité des prescriptions aux points RPI

Attributs	Point de vue			Remarques
	de l'opérateur de réseau téléphonique public	du fournisseur de services	du client de l'abonné de l'utilisateur final	
Disponibilité de service		Elevé	Elevé	
Facturation correcte	Elevé	Elevé		
Taxation correcte			Elevé	
Intégrité du réseau	Elevé			
Intégrité de service		Elevé		
Accès à une adresse de réseau				
Prescriptions liées à la gestion	Elevé	Elevé		

NOTE – Le contenu de ce Tableau n'est pas exhaustif, il pourra être révisé.

BIBLIOGRAPHIE

[B-1] Publication du Secrétariat de l'UIT, *Tendances des réformes dans les télécommunications 2000-2001 – Réglementation de l'interconnexion*.

[B-2] Document de référence de l'OMC sur les télécommunications de base (24 avril 1996) http://www.wto.org/english/tratop_e/serv_e/telecom_e/tel23_e.htm.

[B-3] Principes d'interconnexion de l'APEC (Annexe 3 de [B-1]).

[B-4] Lignes directrices et pratiques de la CITEL en matière de réglementation de l'interconnexion (Annexe 4 de [B-1]).

[B-5] Directive 97/33/CE, "Interconnexion dans le secteur des télécommunications en vue d'assurer un service universel et l'interopérabilité par l'application des principes de fourniture d'un réseau ouvert (ONP)" du Parlement européen et du Conseil du 30 juin 1997.

[B-6] CEPT/ECTRA Recommendation (98)01, *Set of Guidelines on Responsibilities for ensuring maintenance of Network Integrity (NI) in an interconnected environment*.

[B-7] http://www.itu.int/osg/spu/ni/security/links/news.html et http://www.itu.int/osg/spu/ni/security/links/misc.html.

SÉRIES 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	Réseaux câblés et 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, circuits téléphoniques, télégraphie, télécopie 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 de données et communication entre systèmes ouverts
Série Y	**Infrastructure mondiale de l'information, protocole Internet et réseaux de nouvelle génération**
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2004