UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T M.3320

(04/97)

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

SÉRIE M: RGT ET MAINTENANCE DES RÉSEAUX: SYSTÈMES DE TRANSMISSION, DE TÉLÉGRAPHIE, DE TÉLÉCOPIE, CIRCUITS TÉLÉPHONIQUES ET CIRCUITS LOUÉS INTERNATIONAUX

Réseau de gestion des télécommunications

Cadre général des prescriptions de gestion pour l'interface X du réseau de gestion des télécommunications

Recommandation UIT-T M.3320

(Antérieurement Recommandation du CCITT)

RECOMMANDATIONS UIT-T DE LA SÉRIE M

TRANSMISSION DES SIGNAUX RADIOPHONIQUES, TÉLÉVISUELS ET AUTRES SIGNAUX MULTIMÉDIAS

Introduction et principes généraux de maintenance et organisation de la maintenance	M.10–M.299
Systèmes de transmission internationaux	M.300–M.559
Circuits téléphoniques internationaux	M.560–M.759
Systèmes de signalisation à canal sémaphore	M.760–M.799
Systèmes internationaux de télégraphie et de phototélégraphie	M.800–M.899
Liaisons internationales louées par groupes primaires et secondaires	M.900–M.999
Circuits internationaux loués	M.1000–M.1099
Systèmes et services de télécommunications mobiles	M.1100–M.1199
Réseau téléphonique public international	M.1200–M.1299
Systèmes internationaux de transmission de données	M.1300–M.1399
Appellations et échange d'informations	M.1400–M.1999
Réseau de transport international	M.2000–M.2999
Réseau de gestion des télécommunications	**M.3000–M.3599**
Réseaux numériques à intégration des services	M.3600–M.3999
Systèmes de signalisation par canal sémaphore	M.4000–M.4999

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

RECOMMANDATION UIT-T M.3320

CADRE GÉNÉRAL DES PRESCRIPTIONS DE GESTION POUR L'INTERFACE X DU RÉSEAU DE GESTION DES TÉLÉCOMMUNICATIONS

Résumé

La présente Recommandation décrit un cadre général ainsi qu'un ensemble de prescriptions de gestion de base pour la réalisation et l'utilisation de l'interface X du réseau de gestion des télécommunications.

Source

La Recommandation UIT-T M.3320, élaborée par la Commission d'études 4 (1997-2000) de l'UIT-T, a été approuvée le 19 avril 1997 selon la procédure définie dans la Résolution n° 1 de la CMNT.

Mots clés

Aspects internationaux, considérations de sécurité, échange d'informations de gestion, interface X du réseau de gestion des télécommunications (RGT).

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 de la technologie 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 avait/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

Recommandation M.3320

CADRE GÉNÉRAL DES PRESCRIPTIONS DE GESTION POUR L'INTERFACE X DU RÉSEAU DE GESTION DES TÉLÉCOMMUNICATIONS

(Genève, 1997)

1 Introduction

Le présent ensemble de prescriptions définit ce qui est applicable à l'échange d'informations entre Administrations, par l'intermédiaire d'une interface X automatisée d'un réseau de gestion des télécommunications, en vue d'assurer une gestion conjointe du service et du réseau de bout en bout. Il est possible d'élargir ce cadre afin d'y inclure les prescriptions relatives à la gestion de réseau client, qui peuvent ajouter de nouvelles informations à échanger entre Administrations. La présente Recommandation est fondée sur la définition de l'interface X donnée dans la Recommandation M.3010.

1.1 Domaine d'application

La présente Recommandation fait partie d'une série qui traite du transfert d'informations pour la gestion des réseaux et des services de télécommunication. Elle a pour objet de définir un cadre général couvrant toutes les prescriptions liées aux fonctions, aux services et aux réseaux pour l'échange d'informations entre Administrations via le réseau de gestion des télécommunications (RGT). Elle fournit également le cadre général concernant l'utilisation de l'interface X du RGT pour l'échange d'informations entre des Administrations, des exploitations reconnues, d'autres opérateurs de réseaux, des prestataires de services, des clients et d'autres entités.

1.2 Références

1.2.1 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 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.

– Recommandation UIT-T M.3010 (1996), *Principes des réseaux de gestion des télécommunications.*

– Recommandation UIT-T M.3020 (1995), *Méthodologie pour la spécification des interfaces du réseau de gestion des télécommunications.*

– Recommandation UIT-T M.3200 (1997), *Services de gestion du réseau de gestion des télécommunications et domaine géré des télécommunications: aperçu général.*

– Recommandation UIT-T M.3400 (1997), *Fonctions de gestion des réseaux de gestion des télécommunications.*

– Recommandation UIT-T Q.811 (1997), *Profils de protocole de couche inférieure pour les interfaces Q3 et X.*

– Recommandation UIT-T Q.812 (1997), *Profils de protocole de couche supérieure pour les interfaces Q3 et X*.

– Recommandation UIT-T X.160 (1996), *Architecture du service de gestion réseau client pour les réseaux publics de données.*

– Recommandation UIT-T X.161 (1997), *Définition des services de gestion réseau client pour les réseaux publics de données.*

– Recommandation UIT-T X.200 (1994), *Technologies de l'information – Interconnexion des systèmes ouverts – Modèle de référence de base: le modèle de référence de base.*

– Recommandation X.800 du CCITT (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT*.

– Recommandation UIT-T X.811 (1995), *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour systèmes ouverts: cadre d'authentification.*

1.2.2 Autres références

– Recommandation F.435 du CCITT (1991), *Service de messagerie avec échange de données informatisées (EDI).*

– Recommandation M.1520 du CCITT (1992), *Echange normalisé d'information entre Administrations*.

– Recommandation UIT-T M.3000 (1994), *Vue d'ensemble des Recommandations relatives au réseau de gestion des télécommunications.*

– Recommandation UIT-T M.3100 (1995), *Modèle générique d'information de réseau.*

– Recommandation UIT-T X.162 (1997), *Définition des informations de gestion destinées au service de gestion réseau client dans le cadre des réseaux publics pour données à utiliser à l'interface CMNc*.

– Recommandation UIT-T X.163 (1995), *Définition des informations de gestion destinées au service de gestion réseau client dans le cadre des réseaux publics pour données à utiliser avec l'interface CNMe.*

– Recommandation UIT-T X.509 (1997), *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre d'authentification*.

– Recommandation UIT-T X.741 (1995), *Technologies de l'information – Interconnexion des systèmes ouverts – Gestion–systèmes: objets et attributs de contrôle d'accès.*

– Recommandation UIT-T X.802 (1995), *Technologies de l'information – Modèle de sécurité des couches inférieures.*

– Recommandation UIT-T X.803 (1994), *Technologies de l'information – Interconnexion des systèmes ouverts – Modèle de sécurité pour les couches supérieures.*

– Recommandation UIT-T X.810 (1995), *Technologies de l'information – Interconnexion des systèmes ouverts –: aperçu général.*

– Recommandation UIT-T X.812 (1995), *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: contrôle d'accès.*

– Recommandation UIT-T X.813 (1996), *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: non-répudiation*.

– Recommandation UIT-T X.814 (1995), *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: confidentialité.*

– Recommandation UIT-T X.815 (1995), *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: intégrité.*

– Recommandation UIT-T X.816 (1995), *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: cadre d'audit et d'alarmes de sécurité.*

– Norme ISO 9735: 1988 – *Échange de données informatisées pour l'administration, le commerce et le transport (EDIFACT) – Règles de syntaxe au niveau de l'application.*

– Norme ISO 11166-1: 1994 – Banque – *Gestion des clés au moyen d'algorithmes asymétriques – Partie 1: Principes, procédures et formats.*

– Norme ISO 9979: 1991 – *Techniques cryptographiques*. Procédures pour l'enregistrement des algorithmes cryptographiques.

1.3 Abréviations

La présente Recommandation utilise les abréviations suivantes:

AI information d'authentification (*authentication information*)

CMISE élément de service commun de transfert des informations de gestion (*common management information service element*)

CNM gestion de réseau client (*customer network management*)

CPE équipement local d'abonné (*customer premises equipment*)

DAF fonction d'accès à l'annuaire (*directory access function*)

DSF fonction de système d'annuaire (*directory system*)

ER exploitation reconnue

ICF fonction de conversion de l'information (*information conversion function*)

LLA architecture logique répartie en couches (*logical layered architecture*)

MAF fonction d'application de gestion (*management application function*)

MCF fonction de communication de messages (*message communication function*)

OSF fonction des systèmes d'exploitation (*operation system function*)

OSI interconnexion des systèmes ouverts (*open system interconnection*)

RCD réseau de communication de données

RGT réseau de gestion des télécommunications

LAN réseau local (*local area network*)

SF fonction de sécurité (*security function*)

SMK connaissance de gestion partagée (*shared management knowledge*)

WAN réseau régional (*wide area network*)

1.4 Définitions

La présente Recommandation définit les termes suivants:

1.4.1 interface X du réseau de gestion des télécommunications: interface physique appliquée en des points de référence x déterminés (voir la Recommandation M.3010). Le point de référence x est défini comme étant situé entre deux fonctions de système d'exploitation se trouvant sur des RGT différents.

1.4.2 Administration: organisme d'État chargé de représenter l'Etat auquel elle appartient ainsi que les intérêts de celui-ci auprès de l'UIT. À noter qu'il s'agit parfois des PTT et parfois d'un autre organisme. L'entité publique prend alors des mesures visant à administrer sur le plan national les désignations internationales de l'UIT, le numérotage, l'adressage, la comptabilité, etc., en coordination avec l'UIT.

1.4.3 administration: terme pouvant être employé pour désigner, d'une manière générale, des entités qui peuvent posséder ou gérer des réseaux de gestion des télécommunications pour les besoins du service public ou d'un réseau privé.

1.4.4 opérateur de réseau: organisation qui exploite un réseau de télécommunication. Un opérateur de réseau peut être un prestataire de services et vice versa. Il peut ou non fournir des services de télécommunication particuliers.

1.4.5 usager d'un réseau de gestion des télécommunications: entité qui assure au moins un rôle de gestionnaire concernant un réseau de gestion des télécommunications. Dans le contexte d'un RGT, un usager peut se connecter au RGT d'un prestataire de services ou d'un opérateur de réseau par l'intermédiaire de l'interface X, à condition qu'il dispose d'un RGT ou d'un réseau ou système de gestion de type RGT (voir également la Recommandation M.3020).

1.4.6 prestataire de services: terme général désignant une entité qui fournit des services de télécommunication à des clients ou à d'autres usagers sur la base d'un tarif ou par contrat. Un prestataire de services peut ou non gérer un réseau. Il peut ou non être le client d'un autre prestataire de services.

1.4.7 client: organisation ayant une relation commerciale avec un prestataire de services en vue de la fourniture de services de réseau. Ce terme peut désigner un ou plusieurs utilisateurs finals de services de télécommunication.

1.4.8 prescription de gestion: fonction spécifique liée à des entités identifiables. Dans le cadre de l'UIT, ce terme s'applique aux membres de l'UIT qui acceptent par consensus les principes et dispositions énoncés dans la Recommandation de l'UIT.

1.4.9 service de gestion: (voir la Recommandation M.3020).

1.4.10 cas d'accès: dans le contexte de l'interface X, il s'agit de l'ensemble des conditions, des politiques et des facteurs d'environnement commercial dans le cadre duquel l'interface X doit être utilisée.

2 Prescriptions d'architecture et de communication

Le présent paragraphe décrit en détail les prescriptions visant à compléter les profils d'architecture et de protocole de l'interface X du réseau de gestion des télécommunications, mentionnés dans les Recommandations des séries M.3000 et Q.800.

Un système non RGT et un système RGT peuvent communiquer par l'intermédiaire d'une interface X si le premier assure des fonctions RGT et fournit des messages RGT pour cette interface.

2.1 Prescriptions organisationnelles

On peut décrire les différents cas d'accès concernant l'interface X du réseau de gestion des télécommunications en fonction de l'ensemble de conditions, de politiques et de facteurs de l'environnement commercial dans lequel l'interface X doit être utilisée. D'une manière générale, on peut considérer cet ensemble de conditions ou de prescriptions en fonction des organisations qui envisageraient d'utiliser l'interface X du réseau de gestion des télécommunications.

Les prescriptions organisationnelles relatives à la gestion d'un ensemble de ressources sur des RGT ou entre des RGT comportent la subdivision de l'environnement de gestion selon les juridictions, les critères géographiques, les critères technologiques, les politiques, les raisons d'ordre organisationnel et les différents domaines fonctionnels. Les caractéristiques d'une interface X sont principalement définies par les services de gestion de RGT fournis sur cette interface. Toutefois, les considérations examinées dans le présent sous-paragraphe peuvent influer sur les services de gestion fournis par l'intermédiaire d'une interface X ainsi que sur les moyens utilisés pour les fournir.

Il existe différents types de possesseurs de réseaux de gestion des télécommunications, à savoir:

– les Administrations nationales;
– les administrations qui sont des opérateurs de réseaux internationaux;
– les exploitations reconnues de l'UIT;
– les prestataires de services à valeur ajoutée, les organisations industrielles ayant un accès limité aux opérateurs de réseaux locaux/nationaux;
– les clients et les usagers non abonnés.

Au plan administratif, l'interface X peut varier selon les limites géographiques ou juridictionnelles, de la manière suivante:

– à l'intérieur d'une entreprise;
– entre entreprises;
– à l'intérieur d'un pays;
– entre pays.

2.2 Prescriptions organisationnelles en matière d'interfonctionnement

Les différents cas d'accès dans lesquels l'interface X du réseau de gestion des télécommunications peut être utilisée peuvent également être décrits en fonction:

– des prescriptions effectives concernant l'interfonctionnement entre réseaux de gestion des télécommunications;
– de la relation commerciale ou du lien mutuel existant entre possesseurs de réseaux de gestion des télécommunications;
– du type et de la fonction du modèle de gestion susceptible d'être utilisé.

L'ensemble de prescriptions concernant l'interface X du réseau de gestion des télécommunications doit prévoir, entre les RGT, un interfonctionnement qui prend en charge comme suit les différentes applications entre administrations et les différents services commerciaux fournis aux clients:

– interfonctionnement entre RGT publics avec prise en charge de différentes applications entre administrations;
– interfonctionnement entre RGT public et RGT privé avec prise en charge de différents services commerciaux;
– interfonctionnement entre RGT public et réseaux de gestion publics/privés de "type RGT".

Les divers usages de l'interface X du réseau de gestion des télécommunications ont été regroupés dans les modèles suivants. Chaque configuration est considérée comme étant un modèle de gestion unique.

Tableau 1/M.3320 – Classification des modèles de gestion de l'interface X

Modèle de gestion	Relation bilatérale
Modèle de gestion coopérative	Entre deux entités homologues
Modèle de gestion commune	Gestionnaire-Agent
Modèle de gestion de réseau client	Gestionnaire-Agent, Client-Prestataire de services

Les différences entre ces concepts influent sur le traitement des aspects administratifs et des aspects relatifs au contrôle et à la sécurité/définition des profils. Les différences entre les modèles peuvent également faire varier les prescriptions fonctionnelles et les prescriptions du service de gestion.

2.2.1 Modèle de gestion coopérative

Lorsqu'il y a participation de deux opérateurs de réseaux ou plus dans le cadre d'une relation entre entités homologues, le type d'interfonctionnement RGT utilisé sur l'interface X doit être désigné par l'expression "modèle de gestion coopérative".

Le concept de RGT étant destiné à s'appliquer aux réseaux de télécommunication, le possesseur ou l'opérateur du réseau est l'acteur principal de ce réseau dans le cadre d'une relation bilatérale. Dans ce modèle de gestion, un opérateur de réseau doit établir une association avec un autre opérateur par l'intermédiaire de l'interface X du réseau de gestion des télécommunications. En règle générale, il sera nécessaire d'établir un accord bilatéral qui permettra aux deux parties de clairement comprendre et définir les fonctions effectuées sur l'interface X.

Les prescriptions applicables à la gestion coopérative sur l'interface X utilisée entre des entités homologues sont les suivantes:

– il y a participation de deux opérateurs de réseaux ou plus, un ou plusieurs opérateurs pouvant, par ailleurs, assurer ou non le rôle d'un prestataire de services;
– un contrat est requis pour l'établissement de l'interface X et la réalisation des fonctions d'interfonctionnement du RGT;
– un contrat est requis pour chaque service de télécommunication et la gestion de celui-ci;
– les accords bilatéraux peuvent différer selon les parties: par exemple, deux parties peuvent, au sein d'un groupe plus large, négocier des contrats distincts pour l'échange d'informations de gestion par l'intermédiaire de l'interface X;
– une information générale sur la gestion du service est fournie par l'opérateur de réseau lorsque le service est demandé par un ou plusieurs opérateurs;
– chaque partie conserve la maîtrise de ses ressources mais offre aux autres parties, en vertu d'un accord bilatéral, les moyens d'en faire usage;
– deux ou plusieurs opérateurs de réseaux assurent les rôles réciproques de gestionnaire et d'agent.

La Figure 1 montre un exemple de modèle de gestion coopérative.

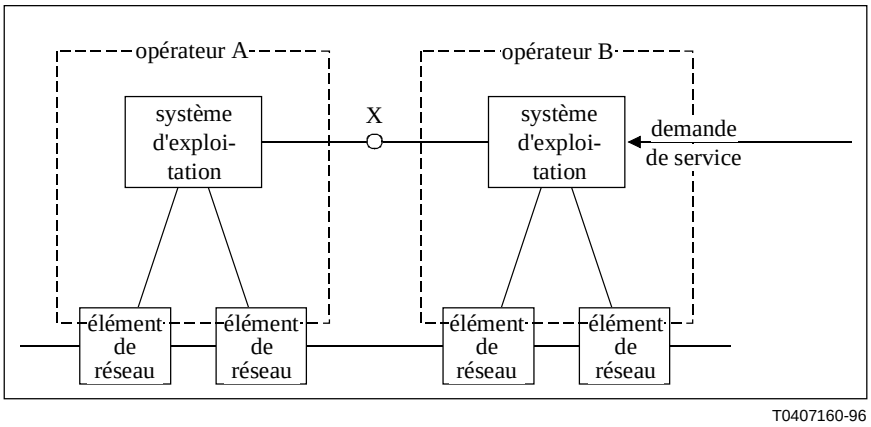


Figure 1/M.3320 – Exemple de gestion coopérative via l'interface X

2.2.2 Modèle de gestion commune

Dans ce modèle de gestion, un groupe d'opérateurs de réseaux peut convenir de centraliser les fonctions en un seul endroit ou en une seule entité opérationnelle. On peut désigner l'expression "gestion commune" ce groupement fonctionnel entre opérateurs de réseaux. D'autres relations bilatérales entre opérateurs peuvent ou non conserver la même forme que dans le modèle coopératif, selon les fonctions qui ont été centralisées. Les fonctions réelles de l'interfonctionnement RGT peuvent ressembler à une configuration constituée d'un seul gestionnaire et de plusieurs agents.

En matière de gestion commune, les arrangements qu'il est possible d'établir grâce à l'utilisation de l'interface X du réseau de gestion des télécommunications peuvent être décrits comme suit:

– deux opérateurs ou plus établissent une entreprise coopérative dans le cadre d'une seule juridiction;
– la contribution et les gains des partenaires sont fonction d'une part convenue des ressources;
– une information générale sur la gestion du service est fournie à un client par un prestataire de services;
– le prestataire de services traite des affaires externes (accords avec des détenteurs non-partenaires) concernant les services de télécommunication convenus;
– les questions de gestion entre l'entité centrale et les ressources des partenaires faisant l'objet d'un contrat sont traitées via l'interface X.

La Figure 2 montre un exemple de modèle de gestion commune.

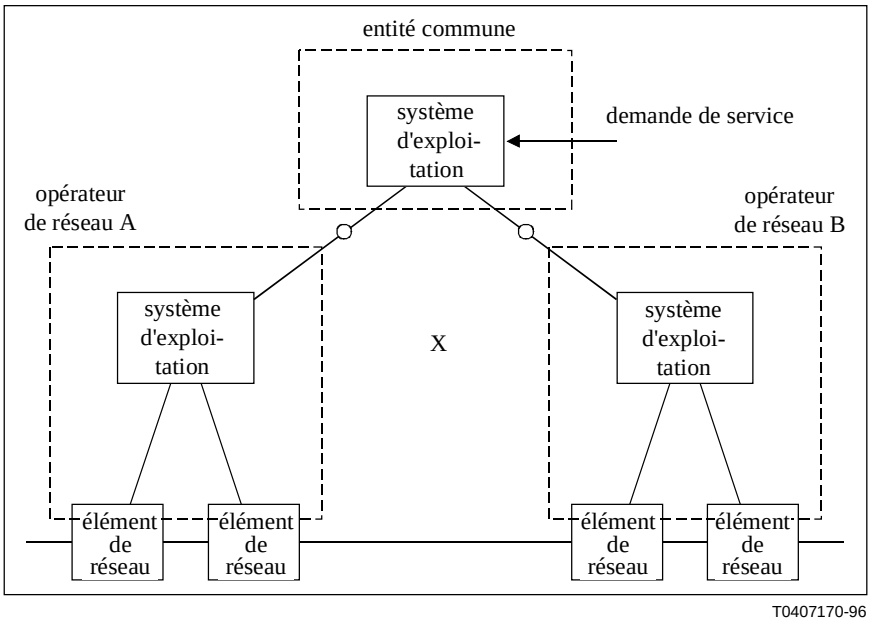


Figure 2/M.3320 – Exemple de gestion commune via l'interface X

2.2.3 Modèle de gestion de réseau client

Un prestataire de services peut fournir des services de gestion à un client sur la base d'un tarif ou conjointement avec l'application d'un tarif, ou encore au titre d'un arrangement commercial. Dans ce cas, l'usager rémunère le prestataire de services et peut donc être désigné par le terme "client". Ce concept, appliqué en association avec l'interface X du réseau de gestion des télécommunications, peut être appelé "gestion de réseau client". Ainsi, on peut désigner cette relation bilatérale par "association prestataire de services-client".

La relation de type prestataire de services-client, réalisée avec le modèle de gestion de réseau client par RGT peut être décrite comme suit:

– il y a participation d'un prestataire de services et d'un client;

– par abonnement, par application d'un tarif ou par contrat, le prestataire de services accorde à un client certains droits de gestion (informations, accès, fonctions, etc.);

– la quantité d'informations fournies et les droits accordés par l'intermédiaire de l'interface X peuvent varier pour chaque contrat de service conclu entre un prestataire de services et chacun de ses clients;

– en règle générale, les clients communiquent au moins en tant que gestionnaires et peuvent assurer des fonctions d'agent selon le domaine d'application du contrat de service particulier conclu avec le prestataire de services.

La Figure 3 montre un exemple de modèle de gestion de réseau client.

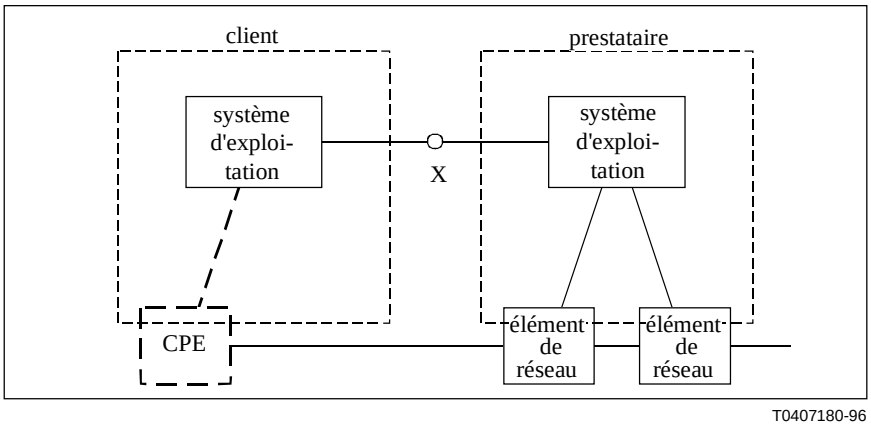


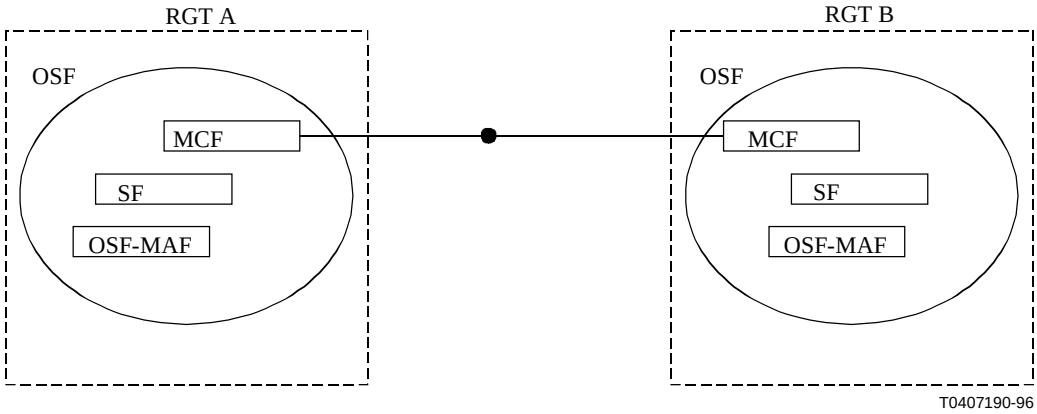
Figure 3/M.3320 – Exemple de gestion de réseau client via l'interface X

A noter qu'un client peut utiliser son propre équipement (CPE) dans son environnement RGT ou "de type RGT".

Lorsque le point de référence x est situé entre un RGT et un système de gestion non RGT, il sera invisible du côté du RGT. Autrement dit, le système non RGT présentera des fonctions de type RGT et prendra en charge les protocoles et les messages RGT.

2.3 Aspects relatifs aux blocs fonctionnels

Le bloc fonctionnel du système d'exploitation au point de référence x du RGT comprendra les composantes fonctionnelles aussi bien obligatoires que facultatives représentées sur la Figure 4.



MAF	fonction d'application de gestion *(management application function)*
MCF	fonction de communication de messages *(message communication fonction)*
SF	Fonction de sécurité *(security function)*
OSF	Fonction de système d'exploitation *(operation system function)*

Figure 4/M.3320 – Blocs fonctionnels du RGT de base aux points de référence x du RGT

2.4 Prescriptions en matière de dénomination et d'adressage

Compte tenu du fait que chaque RGT peut interfonctionner avec plusieurs autres RGT, il est nécessaire que chaque entité gérable soit identifiée de manière indépendante de sa localisation dans les RGT. Il est indispensable que des noms globalement uniques soient attribués à des entités

pouvant être gérées au moyen de relations entre RGT. Il est nécessaire que les entités RGT prenant part à des communications par interfaces X soient capables d'accepter des noms globalement uniques.

Les opérateurs et les utilisateurs de réseau qui utilisent la dénomination globale devront s'assurer de l'unicité de leur nom racine dans le monde entier.

Le format de dénomination globale pour l'interface X du RGT doit comporter les structures suivantes:

– le pays qui doit recevoir le message RGT;
– le nom/code d'organisation qui identifie l'opérateur du réseau international;
– la ressource ou le service identifiés de la même manière qu'à l'intérieur de l'organisation.

Afin de prendre en charge les communications de données entre RGT, on peut utiliser le point d'accès au service de réseau (NSAP, *network service access point*) ou d'autres adresses de couche Réseau pour identifier de manière unique les entités communicantes du système d'extrémité (par exemple, systèmes d'exploitation, éléments de réseau). Les adresses de couche Réseau sont allouées sur une base hiérarchique par l'ISO/UIT-T et peuvent être structurées de manière différente dans les RGT communicants.

Un RGT peut traduire un nom global en adresse de couche Réseau (par exemple, par l'intermédiaire de l'annuaire).

2.5 Services de communication

2.5.1 Aspects relatifs au service interactif

La Recommandation Q.812 définit les services interactifs pour l'interface X du RGT comme étant fournis par l'élément de service commun de transfert des informations de gestion (CMISE, *common management information service element* – voir Recommandation X.710).

L'élément CMISE est organisé sur la base de deux types de services:

– les services de notification de gestion pouvant être utilisés pour signaler tout événement au sujet d'un objet géré, communiqué par l'utilisateur de l'élément CMISE;
– les services d'opération de gestion définissant les opérations de création, extraction, modification, annulation ou exécution d'autres actions sur un objet géré.

2.5.2 Aspects relatifs au service de transfert de fichier

La Recommandation Q.812 définit les services de transfert de fichiers pour l'interface X du RGT comme étant fournis par les parties 1 à 4 de l'ISO 8571 (transfert, accès et gestion de fichiers).

Les structures de fichier prises en charge nécessitent l'utilisation des quatre types de documents suivants:

– fichiers binaires non structurés;
– fichiers de texte structurés;
– fichiers de texte non structurés;
– fichiers ordonnés séquentiellement (ces fichiers sont composés d'une séquence d'enregistrements et ne permettent pas d'accéder directement à un enregistrement donné; chaque enregistrement est constitué de champs de types différents).

2.5.3 Aspects relatifs au service d’annuaire

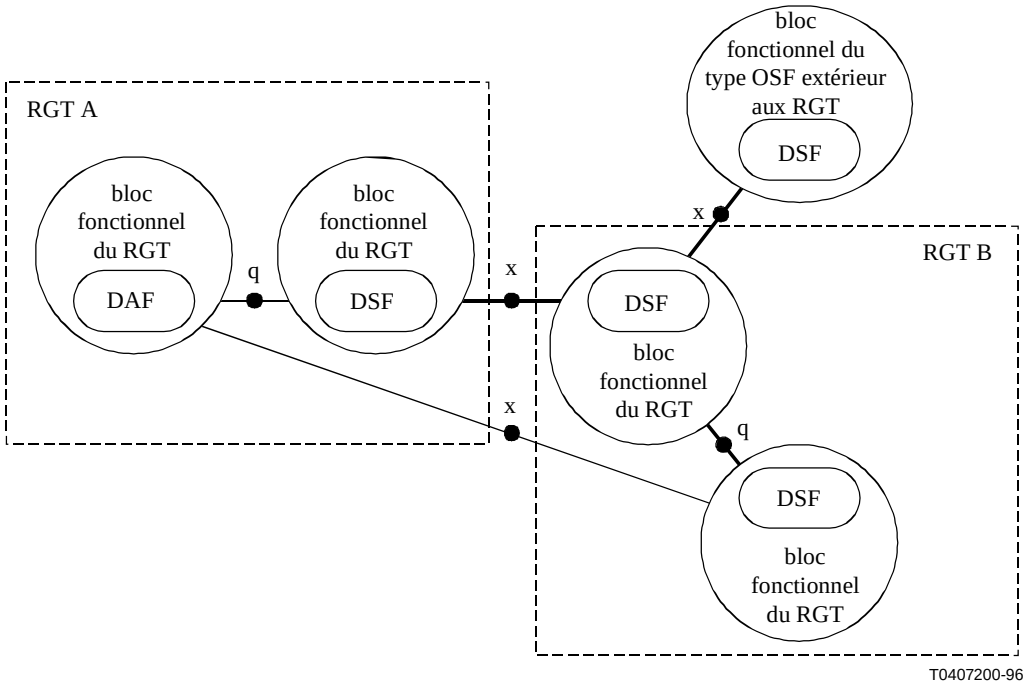
La Recommandation Q.812 définit les services d'annuaire pour l'interface X du RGT comme étant fournis par les Recommandations de la série X.500. Les systèmes d'annuaire permettent de définir

une architecture autorisant la répartition de la base de données de l'annuaire sur un nombre théoriquement illimité de systèmes d'extrémité OSI. En dépit de cette répartition physique, l'utilisateur final ou l'application sollicitant le service d'annuaire doit percevoir l'annuaire comme une entité logique unique.

Les services d'annuaire peuvent être mis en application à travers le point de référence x. La Recommandation M.3010 décrit la relation générale entre les composantes fonctionnelles d'annuaire dans le cadre du RGT. L'extension des services d'annuaire au-delà des limites d'un RGT utilisera le point de référence x. Il est possible d'utiliser ces services chaque fois que la disponibilité globale des informations peut se révéler indispensable au fonctionnement d'un système ou d'un service, ou qu'elle peut améliorer les performances de ces derniers.

A titre d'option, les blocs fonctionnels du RGT peuvent utiliser des composantes fonctionnelles d'annuaire pour implémenter la fonction d'annuaire nécessaire. Cette possibilité est modélisée dans l'architecture fonctionnelle du RGT sous la forme de composantes fonctionnelles du RGT pouvant être contenues dans des blocs fonctionnels spécifiques du RGT, nécessitant des fonctionnalités d'annuaire. La Figure 5 représente l'intégration de l'annuaire et du RGT.

Selon le choix de l'architecture, des associations de fonctions DSF-DSF ou DAF-DSF peuvent être mises en place à travers le point de référence x. Une association peut être établie soit entre les fonctions DSF/DAF des blocs fonctionnels de différents RGT soit entre les fonctions DSF/DAF d'un bloc fonctionnel du RGT et d'un bloc fonctionnel de type RGT extérieur à un RGT spécifique.



composantes fonctionnelles du RGT:

DSF fonction de système d'annuaire *(directory system function)*

DAF fonction d'accès à l'annuaire *(directory access function)*

Figure 5/M.3320 – Architecture d'application d'annuaire à l'interface X du RGT

2.5.4 Aspects relatifs au service d'enregistrement/retransmission

Nécessite un complément d'étude.

2.6 Aspects relatifs au réseau de communication de données

Les différents réseaux de communication de données (RCD) actuellement reconnus pour la prise en charge des interfaces X du RGT sont définis dans la Recommandation Q.811 (Profils de protocole de couche inférieure pour les interfaces Q3 et X). Les types de RCD et la topologie des réseaux seront décidés avec l'accord des propriétaires du RGT sur une base bilatérale ou multilatérale, en tenant compte de la sécurité, de la redondance du réseau et d'autres conditions. Cependant, les concepteurs du RGT peuvent tirer parti des indications décrites dans le présent sous-paragraphe.

Les applications de l'interface X du RGT peuvent utiliser un ou plusieurs profils/piles de protocole de couches inférieures en fonction d'un critère de sélection tel que les performances et la sécurité.

Les prescriptions suivantes du RCD ont été définies pour l'interface X du RGT:

a) les RGT peuvent fonctionner avec une variété de technologies de réseaux dont les WAN (réseau régional) et les LAN (réseau local);

b) les profils de couches inférieures décrits dans la Recommandation Q.811 peuvent être utilisés aux interfaces X;

c) la communication point à point doit être prise en charge pour le transfert global ou interactif de fichier;

d) la communication point à multipoint peut être nécessaire pour satisfaire certaines prescriptions concernant les services de gestion pour quelques domaines gérés;

e) les communications locales, nationales et internationales doivent être prises en charge;

f) l'interconnexion de réseaux permet la communication entre RCD utilisant des protocoles de couche inférieure différents. Les méthodes d'interconnexion de réseaux RCD définies dans la Recommandation Q.811 s'appliquent à l'interface X.

3 Prescriptions relatives au service de gestion

Le présent paragraphe décrit les prescriptions de gestion pour l'utilisation de l'interface X du RGT. Ces prescriptions de gestion devront être structurées correctement pour assurer une interprétation correcte des besoins des utilisateurs du RGT. Les sous-paragraphes suivants sont constitués de façon à répondre aux besoins des utilisateurs. Les aspects internationaux et les aspects relatifs à l'utilisateur sont fournis pour mieux préciser les divers besoins spécifiques des diverses relations.

3.1 Domaines gérés des télécommunications

L'interface X peut prendre en charge l'échange des informations de gestion pour les domaines gérés des télécommunications (tel que défini dans la Recommandation M.3200).

3.2 Relation avec la méthodologie du RGT

Le présent sous-paragraphe doit être considéré comme un cadre général pour les activités de l'interface X du RGT décrites dans les tâches 0, 1 et 2 de la méthodologie du RGT, décrites dans la Recommandation M.3020. Les prescriptions générales pour l'interface X du RGT seront décrites dans le présent sous-paragraphe. Les prescriptions spécifiques pour les services de gestion sont comprises dans les directives pour la définition des services de gestion (GDMS, *guidelines for the definition of management services*), dont le modèle est décrit dans les Recommandations de la série M.3200. Les annexes de la présente Recommandation pouvant traiter des aspects propres au point de référence nécessitent un complément d'étude. Ces prescriptions sont regroupées avec d'autres prescriptions dans des descriptions de services de gestion RGT qui seront ensuite utilisées pour diriger les étapes de planification des bases d'information de tâche X (TIB X).

3.3 Catégories de prescription de gestion

La présente Recommandation définit les prestataires de services qui peuvent offrir des services pour utilisateur final tels que décrits dans les Recommandations UIT-T. Elle reconnaît les opérateurs de réseau qui peuvent exploiter des réseaux comme défini dans les Recommandations UIT-T. Les prestataires de services fournissent des services aux clients et interagissent avec les opérateurs de réseau pour prendre en charge leurs services. (NOTE – La même organisation peut fonctionner à la fois comme opérateur de réseau et comme prestataire de services.)

La gestion de services prise en charge par l'interface X peut être groupée en deux catégories: services applicables entre les rôles et services applicables à l'intérieur d'un même rôle. C'est-à-dire qu'un ensemble de services de gestion peut être défini comme étant applicable entre des opérateurs de réseaux, des prestataires de services et leurs clients, et entre les opérateurs de réseaux et les vendeurs de leurs équipements.

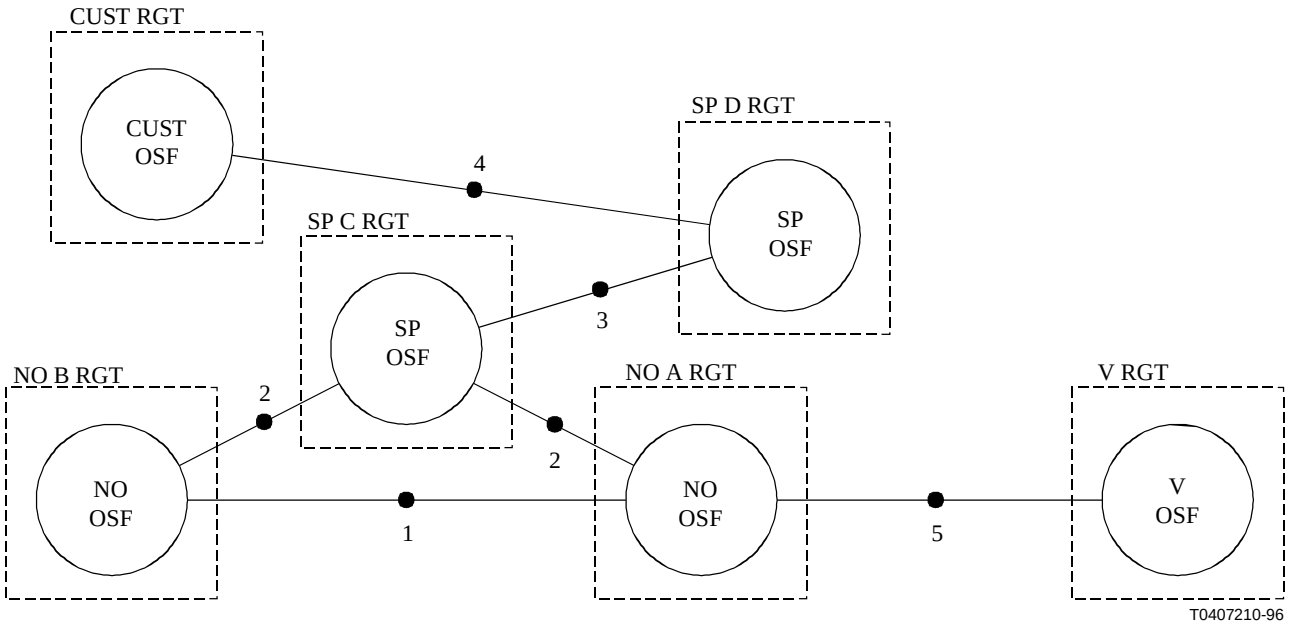
Les interactions entre les participants à ces services de gestion sont caractérisées par les différents modèles de gestion définis dans le paragraphe 2. Elles sont représentées dans le Tableau 2 avec les exemples donnés dans la Figure 6.

Une organisation donnée (propriétaire du RGT) peut agir dans plus d'une seule de ces catégories, c'est-à-dire qu'un opérateur de réseau peut aussi agir comme un prestataire de services. Les prescriptions de gestion peuvent aussi être spécifiées en termes de catégories spécifiques. La raison de l'introduction des catégories de prescription de gestion est la suivante: ces catégories semblent les mieux adaptées pour l'échange d'informations à travers l'interface X.

Il faut noter que, pour une catégorie de prescriptions de gestion donnée, plus d'un modèle de gestion peut être applicable. On adopte par hypothèse les affectations primaires ou secondaires suivantes, mais ces dernières ne sont pas obligatoires.

Tableau 2/M.3320 – Exemples de relations bilatérales

N°	Catégorie de prescription de gestion	Modèles de gestion		
		coopérative	commune	Gestion de réseau client (CNM)
1	Opérateur de réseau - Opérateur de réseau	P	S	S
2	Opérateur de réseau - Prestataire de services	S	S	P
3	Prestataire de services - Prestataire de services	S	S	P
4	Prestataire de services - Client	S	S	P
5	Opérateur de réseau - Vendeur d'équipement	S	S	P*
P option primaire P option primaire en sens inverse S option secondaire				



NO	opérateur de réseau *(network operator)*
SP	prestataire de services *(service provider)*
CUST	client *(customer)*
V	vendeur (de l'opérateur de réseau)
OSF	fonction des systèmes d'exploitation *(operation system function)*

Figure 6/M.3320 – Exemple de relations bilatérales de catégories de gestion

3.3.1 Catégorie de prescriptions de gestion opérateur de réseau – opérateur de réseau

La liste non exhaustive suivante contient les services relatifs aux informations que les opérateurs de réseau peuvent désirer échanger à travers l'interface X afin de tenir compte des procédures existantes entre opérateurs de réseau au moyen d'une interface X du RGT automatisée.

gestion des dérangements (FM, *fault management*):

– gestion des alarmes;
– création de tickets d'anomalie;
– gestion du trafic (partie FM);
– procédure de transfert en escalade;
– essais;

gestion de configuration (CM, *configuration management*)

– gestion du trafic (partie CM);
– point de contact unique;
– administration des clients;
– circuit/configuration du système/mise en service/installation d'un réseau;
– rétablissement;

gestion de la comptabilité (AM, *accounting management*):

– comptabilité;
– échange de facturation;

gestion de la qualité de fonctionnement (PM, *performance management*):

– performance du réseau;

– gestion du trafic (partie PM);

– gestion de la qualité du service;

gestion de la sécurité (SM, *security management*):

– utilisateurs autorisés.

Des priorités ont été données afin d'identifier le besoin le plus urgent pour la prise en charge de l'échange d'informations entre opérateurs de réseau à travers une interface X. La priorité principale est donnée aux spécifications de l'interface X permettant l'utilisation entre opérateurs de réseau. La priorité secondaire portera sur les besoins d'une version client - opérateur réseau de l'interface X.

a) gestion d'erreur pour la commutation et la transmission.

b) maintenance, gestion des dérangements, gestion de la qualité de fonctionnement pour des lignes louées (lignes privées internationales).

c) point de contact unique.

d) mise en service.

e) facturation électronique.

Actuellement, pour un environnement pré-RGT futur, d'autres Recommandations UIT-T définissent l'information échangée entre opérateurs de réseau. Parmi ces Recommandations, la Recommandation M.1520 résume les Recommandations des séries M et E nécessitant un échange d'informations entre opérateurs de réseau. L'interface X du RGT doit satisfaire les prescriptions potentielles d'échange d'informations qui sont actuellement définies. Elle pourra prendre en charge de futures prescriptions supplémentaires par extension des catégories de prescriptions de gestion existantes.

3.3.2 Catégorie de prescriptions de gestion opérateur de réseau – prestataire de services

Les opérateurs de réseau peuvent fournir une interface aux prestataires de services afin:

– de permettre aux prestataires de services d'accéder à l'information sur les ressources du réseau dans les domaines de la gestion des dérangements et de la qualité de fonctionnement;

– de permettre aux prestataires de services de demander à l'opérateur de réseau de prendre en charge un service avec les ressources du réseau dans le domaine de la gestion de configuration et de fournir des informations sur de telles configurations;

– de prendre en charge les fonctions de gestion de comptabilité;

– de prendre en charge les fonctions de gestion de la sécurité.

3.3.3 Catégorie de prescriptions de gestion prestataire de services – prestataire de services

La catégorie de prescriptions de gestion prestataire de services – prestataire de services est nécessaire pour permettre l'échange d'informations de gestion de services entre prestataires de services afin de prendre en charge un environnement commercial donné.

3.3.4 Catégorie de prescriptions de gestion client – prestataire de services

Les clients souhaitent utiliser les possibilités de gestion d'une manière uniforme dans un environnement multi-opérateurs et multiservices afin d'extraire des informations de gestion et de réaliser des opérations de gestion; par exemple l'échange de données concernant les clients, notamment des informations de gestion et de service.

3.3.5 Catégorie de prescriptions de gestion opérateur de réseau – vendeur

Parfois, l'opérateur de réseau est capable de fournir des services de gestion à d'autres entités ne possédant pas ou n'exploitant pas un réseau de télécommunications. Ces entités peuvent être désignées comme étant des utilisateurs tels que le personnel de maintenance du vendeur, les entités contractuelles, etc. Souvent, un contrat de service entre le vendeur et l'opérateur régira les droits et les privilèges dont le personnel de maintenance du vendeur pourra bénéficier concernant les biens de l'opérateur de réseau. Dans ce cas, l'opérateur de réseau doit s'attendre à exécuter le rôle d'agent ou de serveur et l'utilisateur celui de gestionnaire ou de demandeur. Il faut noter que ce modèle peut s'appliquer plus à la maintenance du réseau qu'à la fourniture de service à l'utilisateur final.

3.4 Connaissance de gestion partagée pour l'interface X

Chaque interface du RGT peut être classée suivant le modèle d'informations sur lequel la relation gestionnaire/agent est fondée (voir, en particulier, 3.3 de la Recommandation M.3010: connaissance de gestion partagée). De nombreux modèles d'informations différents seront définis dans le cas de l'interface X, correspondant à des prescriptions fonctionnelles différentes.

La disponibilité d'une telle connaissance de gestion partagée (SMK, *shared management knowledge*) est une condition préalable nécessaire au fonctionnement de l'interface X, et un RGT doit donc fournir ou désigner les moyens pour l'établir.

4 Considérations de sécurité

Le présent paragraphe définit les prescriptions de sécurité pour l'échange d'informations de gestion ainsi que pour la gestion des mécanismes de sécurité qui prendront en charge l'échange des informations de gestion. Le présent paragraphe:

– décrit les conditions qui influenceront nettement le degré de sécurité qui doit ou peut être appliqué dans un cas donné d'utilisation de l'interface X du RGT;

– identifie les dangers et les risques liés aux informations échangées à l'interface X du RGT ainsi que les risques concernant le RGT lui-même;

– identifie les prescriptions fonctionnelles et les capacités de sécurité facultatives qui sont propres à l'interface X du RGT;

– explique les services de sécurité qui seront utilisés sur l'interface X du RGT pour désigner ces dangers, risques et prescriptions identifiés;

– identifie les prescriptions supplémentaires, les caractéristiques et les fonctions pour la gestion des services de sécurité pris en charge par l'interface X du RGT;

– met l'accent sur l'utilisation de l'interface X du RGT pour échanger des clés sans compromettre l'intégrité de l'interface X du RGT elle-même;

– décrit les procédures d'utilisation des algorithmes de chiffrement enregistrés par l'ISO.

4.1 Domaine et objectifs de sécurité

Le présent sous-paragraphe traite uniquement des aspects relatifs à la sécurité propres à l'utilisation, à la maintenance et à la prise en charge de l'interface X du RGT. La présente Recommandation ne définit ni les prescriptions de sécurité pour l'interface Q3 entre système d'exploitation et système d'exploitation ou entre système d'exploitation et élément de réseau ni les prescriptions de sécurité pour les applications et les configurations de l'interface F.

Ces aspects relatifs à la sécurité portent sur la spécification de la composante fonctionnelle du RGT appelée fonction de sécurité, qui est comprise dans la prise en charge du bloc fonctionnel OSF décrit dans la Recommandation M.3010.

Ces aspects relatifs à la sécurité portent aussi sur les services de sécurité du RGT qui entraînent l'échange d'informations entre plusieurs RGT. Ils doivent aussi former la base pour les fonctions de sécurité décrites dans la Recommandation M.3400, sous la rubrique "Fonctions de gestion du RGT" et être considérés comme une prescription pour le service de gestion RGT, "Gestion de la sécurité du RGT".

Le présent sous-paragraphe souligne en détail les prescriptions applicables à l'ensemble de protocoles du RGT pour l'interface X suivant les Recommandations Q.811 et Q.812. Les objectifs de sécurité génériques considérés pour l'interface X du RGT incluent l'authentification, le contrôle d'accès, la confidentialité, la non-répudiation de l'intégrité et les audits de sécurité.

4.1.1 Considérations relatives à l'application

Chaque application de l'interface X doit être étudiée en détail dans le cadre de la méthodologie d'interface du RGT, afin de déterminer la meilleure manière de résoudre les questions relatives aux dangers, aux risques et aux prescriptions de sécurité.

Tous les mécanismes de sécurité ne sont pas nécessaires pour chaque application. Une application peut utiliser un modèle particulier de gestion de l'interface X du RGT. Elle peut comprendre un ou plusieurs services de gestion du RGT, un ou plusieurs ensembles de fonctions de gestion et une ou plusieurs fonctions de gestion du RGT. Les services de communications et les conditions d'environnement nécessitent d'être regroupés dans les décisions prises au niveau de la sécurité utilisée pour l'interface X. Chaque service de gestion fourni par une application de l'interface X du RGT doit être décomposé jusqu'au niveau fonctionnel avant la prise de décision sur les prescriptions de sécurité.

4.1.2 Considérations relatives à l'implémentation

Les politiques de sécurité peuvent être différentes entre les Administrations de différents pays. Qui plus est, une même Administration peut ne pas avoir les mêmes pratiques de sécurité que d'autres Administrations. On ne doit donc pas partir du principe que les prescriptions de sécurité peuvent être imposées aux différents pays qui voudront utiliser l'interface X du RGT.

Les politiques de sécurité qui peuvent différer de pays à pays peuvent comporter des valeurs admissibles pour les mécanismes d'authentification, pour les types, ou les puissances de chiffrement, pour les techniques cryptographiques utilisées ou pour les longueurs de clés de chiffrement, etc.

Des procédures d'interfonctionnement supplémentaires peuvent être nécessaires pour surmonter les limitations pratiques ou d'un autre ordre qui peuvent résulter de différences entre politiques de sécurité, entre technologies de système de sécurité et entre réseaux de communication de données. Des prescriptions de sécurité supplémentaires peuvent être utiles dans une implémentation particulière.

Les considérations de sécurité d'implémentation qui doivent être regroupées dans la solution de sécurité pour une implémentation particulière de l'interface X comprennent:

– les politiques nationales de sécurité;
– la technologie de sécurité mise à la disposition de différents pays;
– la configuration des réseaux de communications de données; des réseaux commutés par rapport aux réseaux spécialisés;
– les réseaux de données commutés publics par rapport aux réseaux de données commutés privés;

– le nombre de réseaux ou de noeuds intermédiaires utilisés dans la configuration des RCD;
– le type et la configuration des RCD tels que SS7, OSI/X.25, TCP/IP, LAN/WAN, RNIS, etc.

4.2 Menaces

Une analyse approfondie de toutes les menaces qui peuvent être rencontrées doit être faite.

Les menaces décrites dans la présente Recommandation sont fondées sur les concepts définis dans les ISO 7498-2 et ISO/CEI 10181. Les menaces qui peuvent entraîner des risques de sécurité sont décrites dans les paragraphes suivants.

4.2.1 Divulgation d'information

Les menaces relatives à la confidentialité des informations sont l'accès à l'information par une entité non autorisée. L'information peut être acquise illégalement par une entité non autorisée. Il s'agira par exemple de l'interception de messages en transit ou de l'accès non autorisé à des informations contenues dans des systèmes.

Exemple:

– la divulgation d'unités de données du protocole commun des informations de gestion (CMIP, *common management information protocol*) ou d'un autre protocole, sans autorisation propre ou à destination d'utilisateurs non autorisés.

4.2.2 Accès non autorisé

Cette menace comprend l'accès non autorisé aux systèmes et aux ressources qui y sont contenues, comme les données et les logiciels. Une fois que l'accès non autorisé est acquis à travers l'interface X, les dommages résultants pourront interrompre le fonctionnement normal du système. Des informations importantes et confidentielles pourront être perdues, modifiées, ou divulguées, pouvant finalement remettre en cause des opérations commerciales.

4.2.3 Usurpation

Cette menace est la simulation d'une entité par une autre entité différente afin d'accéder à l'information ou à des privilèges supplémentaires.

4.2.4 Menaces relatives à l'intégrité des informations

Les menaces relatives à l'intégrité des informations comprennent tant la production non autorisée ou la modification de l'information contenue dans les systèmes que l'information en transit. Par exemple, la réexécution, la copie, le réagencement, l'insertion, la suppression, la création, la modification de données avant ou durant la transmission.

4.2.5 Refus de service

Le refus de service survient lorsqu'une entité échoue dans l'exécution de sa fonction ou empêche d'autres entités de remplir leur fonction. Cela peut comprendre le refus de l'accès au RGT, le refus de la communication dû à l'encombrement du RGT. Dans un réseau partagé, ce danger peut être reconnu comme une production de trafic excédentaire encombrant le réseau, empêchant d'autres usagers de l'utiliser en retardant leur trafic.

4.2.6 Répudiation

Refus d'une des entités impliquées dans une communication de reconnaître avoir participé entièrement ou en partie à la communication.

4.2.7 Fraude

Un utilisateur non autorisé qui utilise ou dévie une ressource ou un service, entraînant la perte d'un ou de plusieurs utilisateurs du RGT, commet une fraude. La fraude est spécialement critique dans le cas de la gestion de client car elle compromet l'exactitude de la facturation et de l'acheminement d'un service.

4.3 Prescriptions de sécurité

Des risques existent lorsqu'un ou plusieurs RGT ou RCD fournissant l'interface X sont exposés à un ou à plusieurs dangers. La première étape pour contrer les dangers est de faire une évaluation des risques. L'appendice I illustre une méthode d'évaluation de la sécurité.

4.3.1 Prescriptions d'identification

Les RGT doivent offrir des capacités adéquates pour l'identification des utilisateurs dans l'environnement RGT. Ces capacités peuvent être nécessaires pour prendre en charge l'aptitude à la vérification de toutes les actions et activités des utilisateurs dans le réseau et pour fournir les données d'entrée d'authentification et de contrôle d'accès.

Les prescriptions de sécurité de base pour l'identification peuvent être les suivantes:

– les utilisateurs du réseau doivent avoir des noms ou des identifiants globalement sans ambiguïté aux fins d'identification, afin de prendre en charge individuellement leurs aptitudes à la comptabilité et à la vérification;

– un RGT doit envoyer (faire suivre) le nom d'utilisateur ainsi que l'identificateur RGT dans les communications traversant des domaines ou des frontières de juridiction.

4.3.2 Prescriptions de secret

Les prescriptions de secret doivent être prises en charge pour assurer que les informations confidentielles ne sont pas compromises. Les prescriptions de secret de base peuvent être les suivantes:

– un RGT doit avoir la capacité de chiffrer les informations confidentielles communiquées à l'intérieur d'un même RGT ou entre plusieurs RGT, ainsi que les informations confidentielles stockées à l'intérieur d'un même RGT;

– un RGT doit avoir la capacité d'assurer de bout en bout la confidentialité des données communiquées à l'intérieur d'un même RGT ou entre plusieurs RGT;

– un RGT doit chiffrer les informations confidentielles lors de l'utilisation d'une technique de diffusion;

– un RGT doit avoir la capacité de garantir la distribution et la gestion des clés.

4.3.3 Prescriptions d'authentification

Les RGT doivent offrir des capacités adéquates pour permettre la légitimation des utilisateurs. Contrairement à d'autres, certaines de ces capacités sont génériques par nature et sont indépendantes du type de mécanisme d'authentification en pratique.

L'authentification est une prescription obligatoire lorsque les dispositions du réseau commuté sont utilisées entièrement ou en partie pour réaliser une interface X du RGT. Pour les configurations de réseau spécialisées de bout en bout où les identités des deux correspondants du RGT sont certaines, l'authentification peut être considérée comme facultative.

Les prescriptions pour l'authentification peuvent être les suivantes:

– un RGT doit avoir la capacité d'authentifier les utilisateurs;
– un RGT ne doit pas prendre en charge les moyens de court-circuiter le mécanisme d'authentification;
– la confidentialité de toutes les informations secrètes d'authentification doit être préservée par un RGT. Lorsque l'information d'authentification (AI, *authentification information*) est stockée à l'intérieur d'un RGT, elle doit être protégée contre des accès non autorisés. Certaines informations d'authentification (par exemple, mot de passe chiffré) ne doivent pas être disponibles en clair, même pour les utilisateurs à haut niveau de privilèges;
– chaque utilisateur du RGT doit avoir une information d'authentification unique;
– cette information d'authentification ne doit pas être envoyée en texte clair à l'intérieur d'un même RGT ou entre plusieurs RGT, sauf si cela est imposé par un mécanisme d'authentification particulier en cours d'utilisation; par exemple des mots de passe à usage unique ou certains mécanismes de question rédhibitoire-réponse;
– l'intégrité de toutes les informations d'authentification à stockage interne doit être préservée par un RGT;
– un RGT doit avoir la capacité de fournir une authentification efficace des utilisateurs souhaitant exécuter des fonctions administratives "critiques" et d'autres fonctions de gestion, exploitation, maintenance et mise en oeuvre;
– un RGT doit avoir la capacité d'intégrer et de prendre en charge des procédés d'authentification, y compris ceux qui sont fondés sur des accords bilatéraux simples, sur des serveurs de tiers habilités et sur des mots de passe simples.

Il faut noter que les systèmes et configurations d'habilitation sont considérés comme relevant de l'implémentation et de négociations bilatérales. Certains modèles de gestion peuvent nécessiter l'utilisation de tiers habilités. En revanche, le modèle de gestion coopérative peut dépendre seulement d'accords bilatéraux.

4.3.4 Prescriptions de contrôle d'accès

Les RGT doivent avoir les capacités de gérer (accorder ou refuser) l'accès aux diverses ressources de télécommunication en fonction d'identités d'utilisateur authentifiées correctement. Les prescriptions pour l'utilisation des procédures de contrôle d'accès dépendent du service de gestion offert en pratique. Les directives pour l'utilisation du contrôle d'accès sur l'interface X du RGT peuvent être les suivantes:

– un RGT ne doit pas permettre aux utilisateurs d'accéder à des ressources de système ou de réseau s'ils ne sont pas correctement identifiés et authentifiés;
– un RGT doit offrir la capacité de contrôler l'accès aux ressources du RGT à tous les niveaux de granularité;
– un RGT doit avoir la capacité d'intégrer et de prendre en charge la fourniture du contrôle d'accès à diverses classes d'utilisateurs y compris les utilisateurs particuliers, les groupes, les rôles et les mandataires;
– un RGT doit avoir la capacité de filtrer l'accès aux ressources sur la base d'une combinaison quelconque des éléments suivants: entité expéditrice/adresse du demandeur, opération demandée, entité destinataire/adresse de destination ainsi que sur la base d'un profil d'autorisation;

– un RGT doit avoir la capacité d'intégrer et de prendre en charge des mécanismes pour accorder ou refuser l'accès aux utilisateurs en fonction de l'information contextuelle (par exemple le temps);
– un RGT doit avoir la capacité de contrôler l'accès aux applications qui effectuent l'acheminement, la configuration et la commande de débit.

4.3.5 Prescriptions d'intégrité

Les prescriptions de base pour l'intégrité du réseau, des données et du système peuvent être les suivantes:

– un RGT doit avoir la capacité d'associer correctement n'importe quelle ressource de réseau (données, processus) avec son créateur/propriétaire initial. Des dispositions spécifiques doivent être prises pour prendre en charge l'anonymat de l'utilisateur;
– un RGT doit associer correctement les données communiquées avec leur origine;
– un RGT doit avoir la capacité d'assurer l'intégrité de bout en bout des données communiquées à l'intérieur d'un même RGT ou à travers plusieurs RGT;
– un RGT doit offrir des mécanismes de protection contre les attaques par réexécution;
– un RGT doit préserver l'intégrité des données RGT.

4.3.6 Prescriptions relatives aux audits de sécurité

Les prescriptions de base relatives aux audits de sécurité peuvent être les suivantes:

– un RGT doit offrir les moyens de valider le fonctionnement correct des mécanismes de sécurité (par exemple, activation de la journalisation de sécurité);
– le journal de sécurité, la commande de vérification ainsi que d'autres fonctions de sécurité fournies à l'intérieur du RGT, doivent survivre aux redémarrages.

4.4 Services de sécurité

La solution de sécurité pour une application d'interface X du RGT particulière doit comprendre un profil de sécurité. Celui-ci englobe l'ensemble des prescriptions qui ont été estimées applicables et nécessaires pour contrer les dangers et pour minimiser les risques. Les services de sécurité seront déterminés d'après les prescriptions d'application de la manière suivante:

Tableau 3/M.3320 – Prescriptions et services de sécurité

Prescription	Service de sécurité
identification et authentification	authentification de l'utilisateur authentification de l'entité homologue authentification de l'origine des données
contrôle d'accès et authentification	contrôle d'accès authentification de l'origine des données
contrôle d'accès et authentification	contrôle d'accès
intégrité – données stockées	contrôle d'accès détection de refus de service
intégrité – données transférées	intégrité détection de refus de service
confidentialité – données stockées	contrôle d'accès réutilisation d'objet [a)]

Tableau 3/M.3320 – Prescriptions et services de sécurité *(fin)*

Prescription	Service de sécurité
confidentialité – données transférées	confidentialité réutilisation d'objet
non-répudiation	non-répudiation
(tout)	alarme de sécurité, piste de vérification, reprise
[a] Le terme "réutilisation" d'objet désigne un service de sécurité garantissant que les supports de stockage (mémoire, disque, bande, etc.) ne conservent aucune information résiduelle après utilisation.	

4.4.1 Services d'authentification

L'authentification fait généralement référence à l'authentification de l'entité homologue au moment de l'établissement de l'association; mais elle peut aussi faire référence à l'authentification de l'utilisateur et/ou à l'authentification de l'origine des données. L'authentification de l'utilisateur n'effectue qu'une légitimation de l'identité de l'utilisateur qui est, le plus vraisemblablement, l'initiateur de l'association.

L'authentification de l'entité homologue durant l'établissement de l'association peut être à sens unique ou bilatérale. L'authentification à sens unique indique uniquement l'initiateur de l'association, tandis que l'authentification bilatérale authentifie à la fois l'identité de l'initiateur et celle du destinataire de l'association.

Le service d'authentification de l'origine des données fournit la légitimation de la source d'une unité de données. Le service n'assure pas la protection contre la duplication ou la modification des unités de données.

4.4.2 Services de contrôle d'accès

Ce service assure la protection contre des opérations non autorisées d'accès, d'utilisation, de lecture, d'écriture et de suppression d'informations. Il permet l'exécution d'une ressource de traitement ou de tous les accès à une ressource.

L'utilisation des services de contrôle d'accès dépend de spécificités identifiées dans les services de gestion du RGT étant donné qu'aussi bien les informations que les ressources varieront suivant les fonctions exécutées. Les mécanismes de contrôle d'accès qui peuvent être utilisés sont les suivants:

– des listes de contrôle d'accès indiquant les droits d'accès d'entités homologues;
– l'échange de renseignements identifiant les informations et les ressources qui peuvent être autorisées;
– l'échange d'informations d'authentification telles que des mots de passe;
– des étiquettes de sécurité indiquant le niveau de sensibilité de données élémentaires, qui peuvent être utilisées pour accorder ou refuser l'accès (il est souvent nécessaire d'acheminer l'étiquette de sécurité avec les données en transit);
– la journalisation de l'heure d'accès, de l'itinéraire de tentative d'accès, de la durée d'accès et du suivi de l'utilisation des ressources.

4.4.3 Services de confidentialité

Des différentes formes de services de confidentialité, deux peuvent servir à assurer le secret des transactions au niveau de l'interface X:

– la confidentialité de la connexion assurera un chiffrement total du train de données;

– la confidentialité des données de message, y compris la confidentialité sélective des champs, peut servir à protéger la confidentialité des données intervenant dans les transactions au niveau de l'interface X.

L'utilisation des services de confidentialité doit être facultative et être soumise à des accords bilatéraux et à un respect des politiques de sécurité.

4.4.4 Intégrité des données

L'intégrité des données contre les dangers en cours, en assurant l'intégrité de tous les champs de données sélectionnés et en détectant toute modification, insertion, suppression ou réexécution de données quelconque à l'intérieur d'une séquence entière.

Les services d'intégrité des données comprennent:

– *l'intégrité sélective de champs*: ce service peut être fourni dans la couche Application ou dans le processus d'application lui-même, étant donné que c'est uniquement le processus d'application qui peut différencier les champs;

– *l'intégrité en mode connexion*: ce service peut être fourni dans la couche Transport, dans la couche Application ou dans le processus d'application;

– *l'intégrité en mode connexion sans reprise*: ce service peut être fourni dans la couche Réseau, dans la couche Transport, dans la couche d'Application ou dans le processus d'application.

4.4.5 Non-répudiation

Ce service fournit au destinataire des données la preuve de l'origine des données et à l'expéditeur la preuve de la remise des données.

4.5 Gestion de la sécurité

4.5.1 Prescription de vérification

Les RGT doivent offrir les capacités adéquates pour permettre la recherche, la vérification et la détection en temps réel ainsi que pour analyser les activités afin que des mesures correctives adéquates puissent être prises.

4.5.2 Piste de vérification

La piste de vérification de sécurité permet de consigner les événements liés à la sécurité qui peuvent éventuellement être utilisés dans une vérification de sécurité. La piste de vérification de sécurité doit être réalisée au moyen de journaux de sécurité de la manière suivante:

– des journaux de sécurité doivent être établis et conservés à l'intérieur du RGT (par exemple avec une protection contre une défaillance du système);

– les journaux de sécurité seront protégés contre les accès non autorisés et aucune modification ne devra être permise;

– les journaux de sécurité enregistreront au moins les événements suivants: tentatives non valides d'authentification de l'utilisateur, tentatives non autorisées d'accès à des ressources

RGT de type quelconque, modification des droits d'accès d'un utilisateur, reprise après arrêt, suppressions de journaux, modification des attributs de sécurité associés à une ressource RGT;

– pour chaque événement enregistré, les journaux de sécurité comprendront au moins les paramètres suivants: date et heure de l'événement en temps universel coordonné (UTC, *universal time coordinated*), identité d'utilisateur incluant l'adresse réseau (s'il y a lieu), type d'événement, noms des ressources RGT atteintes, succès ou échec de l'événement.

– journalisation de violations de sécurité apparentes et journalisation des événements "normaux" (ouverture d'une session, par exemple). Pour plus de précisions, voir les Recommandations X.816, X.735, X.736 et X.740.

La Recommandation UIT-T X.740 définit un modèle pour produire les rapports de piste de vérification de sécurité. Les prescriptions énumérées plus haut sont conformes à la Recommandation X.740.

4.5.3 Signalisation des alarmes

Les alarmes de sécurité constituent un type particulier de rapport d'événement qui doit toujours être consigné. La signalisation des alarmes de sécurité est utilisée pour signaler à une entité une violation ou une tentative de violation de la sécurité. Les Recommandations suivantes s'appliquent:

– Recommandation X.734 du CCITT (1992), *Technologies de l'information – Interconnexion des systèmes ouverts – Gestion-systèmes: fonction de gestion des rapports d'événement;*

– Recommandation X.736 du CCITT (1992), *Technologies de l'information - Interconnexion des systèmes ouverts – Gestion-systèmes: fonction de signalisation des alarmes de sécurité.*

Un RGT doit offrir un mécanisme pour signaler à l'administrateur (par exemple, par alarme, par rapport en ligne) en temps réel si possible, un échec d'enregistrement des événements qu'il faut absolument enregistrer dans le journal de sécurité.

Un RGT doit offrir la capacité de transférer les informations de vérification sur un support de stockage permettant une plus longue conservation: la réécriture doit être interdite.

4.5.4 Prescriptions administratives

Il y a un certain nombre de fonctions administratives que le RGT doit prendre en charge séparément des autres fonctions d'utilisateur.

Puisque de nombreux problèmes de sécurité peuvent impliquer plusieurs RGT interconnectés, il est parfois souhaitable qu'un RGT transmette des informations utiles concernant ces événements. Sinon les prescriptions citées ci-dessous peuvent s'appliquer simplement au RGT lui-même, au lieu d'être limité à la seule interface X du RGT:

a) un RGT doit offrir un mécanisme permettant à un administrateur chargé de la sécurité d'afficher tous les utilisateurs actifs à un moment donné;

b) un RGT doit offrir un mécanisme permettant à l'administrateur chargé de la sécurité de visualiser séparément et sélectivement les actions de n'importe quel utilisateur, y compris les utilisateurs privilégiés en fonction de l'identité individuelle de chaque utilisateur;

c) un RGT doit offrir un mécanisme permettant à l'administrateur chargé de la sécurité de bloquer un conduit de communication spécifique en gérant l'accès aux passerelles et aux systèmes de relais intermédiaire;

d) un RGT doit offrir des commandes de protection contre les encombrements aussi bien automatiques que manuelles afin de contrer les attaques par refus de service; par exemple,

attaques par encombrement intentionnel pouvant empêcher le RGT d'effectuer des actions et des réponses en temps utile;

e) un RGT doit offrir, en cas de défaillance de sécurité, la capacité de maintenir ou de rétablir en temps utile les services réseau des fonctions de gestion, exploitation, maintenance et mise en oeuvre; par exemple en fournissant la capacité de récupérer les données et de réinitialiser le système;

f) un RGT doit offrir à l'administrateur chargé de la sécurité la capacité d'inactiver les identificateurs d'utilisateur qui n'ont pas été utilisés pour une période spécifiable ou pour d'autres besoins administratifs spécifiques;

g) un RGT doit offrir à l'administrateur chargé de la sécurité un mécanisme permettant de réinitialiser les informations d'authentification des utilisateurs ou de supprimer des comptes d'utilisateurs;

h) un RGT doit offrir la capacité de produire les alarmes pour des événements de sécurité spécifiables y compris les violations d'intégrité (par exemple les réexécutions), et les violations physiques (par exemple, manipulation frauduleuse d'un câble et éléments d'intrusion);

i) un RGT doit offrir à l'administrateur chargé de la sécurité des outils d'analyse de vérification après collecte d'informations qui pourront produire des rapports d'anomalie, des rapports récapitulatifs, et des rapports détaillés sur des éléments de données spécifiques du réseau et sur des utilisateurs;

j) un RGT doit aussi protéger les outils opérationnels contre les accès non autorisés.

4.5.5 Gestion de clés

La sécurité commence par la disponibilité et l'utilisation de clés de chiffrement. La gestion de clés fait référence à la production, au stockage, à la distribution, à la suppression, à l'archivage et à l'application de clés conformément à une politique de sécurité qui peut être définie par l'ensemble des critères de fourniture de services de sécurité. La gestion de clés représente donc une première étape critique pour fournir et garantir des services de sécurité fiables.

La Recommandation Q.812, Profils de protocole de couches supérieures pour les interfaces Q3 et X, identifie les mécanismes spécifiques de protocole de sécurité à appliquer sur l'interface X du RGT. Par opposition, la présente Recommandation spécifie uniquement les prescriptions de gestion pour le traitement des clés à l'interface X du RGT. De plus, la présente Recommandation spécifie les prescriptions pour l'utilisation de l'interface X du RGT, sur une base facultative, pour la distribution ou l'échange de clés de chiffrement.

4.5.6 Prescriptions

Les deux parties de l'interface X du RGT doivent être capables de prendre en charge la gestion de clés car les clés de chiffrement seront nécessaires pour assurer les divers services de sécurité cités précédemment. Les prescriptions minimales pour la gestion de clés sont les suivantes:

– contrôle des clés durant leur durée de vie pour empêcher une divulgation, une modification, ou une substitution non autorisée;

– distribution des clés afin de permettre l'interfonctionnement d'équipements ou d'installations de chiffrement;

– confirmation de l'intégrité des clés durant toutes les phases de leur vie, y compris leur production, leur distribution, leur stockage, leur introduction, leur utilisation et leur destruction;

– récupération, en cas de défaillance des processus de gestion de clés, lorsque l'intégrité des clés est mise en question.

La gestion de clés peut être exécutée manuellement ou automatiquement. La gestion de clés manuelle correspond généralement à la distribution des clés aux endroits où elles sont nécessaires, à l'aide de certaines procédures manuelles (courrier recommandé, courrier sous pli cacheté, bande magnétique, etc.). Par opposition, la gestion de clés automatique permet aux clés d'être transmises de manière électronique à des endroits appropriés par certains canaux de communication fiables. Toutefois, il faut noter que même si la gestion automatique des clés est acceptée, il faudra toujours une prise en charge de procédures manuelles pour l'action "d'amorçage" afin d'établir la première et la plus importante connexion sûre.

La gestion de clés varie aussi en fonction du système de chiffrement utilisé dans une application particulière de l'interface X du RGT. Il existe deux types de systèmes de chiffrement décrit ci-dessous: clé privée et clé publique.

4.5.7 Gestion de clés privées

Le premier type de gestion de clés prend en charge les systèmes de chiffrement à clés privées qui utilisent une transformation secrète (clé) pour chiffrer les données envoyées par un canal de communication. La même clé est utilisée dans le RGT récepteur pour reconvertir les données chiffrées dans leur forme originale. La clé de transformation est envoyée au destinataire autorisé par un canal fiable et les autres destinataires n'y ont donc pas accès.

Les systèmes de clés privées dépendent de la distribution des données de clés privées, effectuée de façon manuelle ou automatique, par un canal fiable. Ce canal peut être une interface X du RGT. La méthode du système de clés privées permet de limiter la sécurité aux deux RGT impliqués dans l'échange d'informations indépendamment des informations échangées avec d'autres RGT. Ce caractère bilatéral du système de clés privées est intéressant pour les applications utilisant le modèle de gestion coopérative.

On pourra se reporter à l'appendice II pour de plus amples informations.

4.5.8 Gestion de clés publiques

Le deuxième type de chiffrement implique l'emploi de systèmes de chiffrement à clés publiques utilisant des clés distinctes aux stations d'émission et de réception. L'une des clés est rendue publique et l'autre est gardée secrète. Cette dernière ne peut pas être calculée à partir de la clé publique. Chaque RGT, dans une relation bilatérale ou dans un groupe, aura besoin de garder secrète sa clé privée et divulguera l'autre. Ces clés peuvent alors être utilisées dans diverses transformations de sécurité.

4.5.9 Systèmes d'habilitation

L'interface X doit être capable de prendre en charge les interactions avec des tiers habilités pour l'authentification, la certification et la distribution de clés.

4.6 Chiffrement de données

Les participants aux interactions de l'interface X doivent être capables d'utiliser un registre de chiffrement tel que l'ISO 9979. L'exemple d'un registre cryptographique est traité dans l'appendice III.

APPENDICE I

Informations supplémentaires sur l'évaluation des risques

Pour contrer les différentes menaces, les participants aux services d'interface X peuvent effectuer une analyse des risques dans le but de:

– fournir une évaluation des différents dangers;

– identifier les risques en fonction des dangers correspondants;

– donner la priorité aux risques nécessitant une analyse et définir la fréquence de cette analyse;

– établir un rapport d'évaluation des risques.

Le rapport d'évaluation des risques devient la base de l'analyse ultérieure des risques, dans laquelle chaque risque sera étudié plus en détail pour déterminer:

– la probabilité qu'un point faible soit détecté;

– le prix et l'effort nécessaires pour exploiter le point faible;

– le bénéfice pouvant être retiré par l'intrus en exploitant le point faible;

– les dommages potentiels pour les intérêts de la compagnie d'exploitation ou pour les abonnés de la compagnie.

Les résultats de l'analyse des risques doivent fournir assez d'informations pour que les planificateurs de l'interface X du RGT soient en mesure de mettre au point une solution de sécurité permettant de contrer les dangers et de minimiser les risques. La solution de sécurité doit comprendre un profil de sécurité pour chaque application particulière de l'interface X du RGT, en tenant compte aussi bien de cette application que des considérations d'implémentation décrites précédemment.

APPENDICE II

Informations supplémentaires sur la gestion de clés privées

Les grandes lignes suivantes décrivent les prescriptions minimales pour fournir un système de gestion de clés privées qui utilise l'interface X du RGT en tant que canal fiable:

– une clé principale est manuellement partagée entre les administrateurs des deux RGT et représente la première étape d'un processus composé de trois étapes. La clé principale est également appelée "clé chiffrant d'autres clés" (KEK, *key encrypting key*);

– cette clé principale est utilisée pour chiffrer un deuxième niveau de clés, appelé "clés de session" ou "clés de chiffrement de données" (DEK, *data encrypting key*);

– les clés de session sont disséminées de manière électronique par canal de communication fiable, tel que l'interface X du RGT. Les clés peuvent être disséminées au moyen d'un des services de communication de l'interface X du RGT. Toutefois, dans la plupart des cas, l'échange sera simplement un transfert de fichier;

– les clés de session sont utilisées par les deux RGT pour chiffrer les champs sélectifs ou les messages de données selon les services de sécurité nécessaires pour chaque application de l'interface X du RGT;

– dans certaines installations, des besoins supplémentaires peuvent exister pour chiffrer les fichiers contenant les clés de session au moyen d'un troisième ensemble de clés appelé "clés d'installation". Toutefois s'il n'existe pas de risque apparent lorsque les clés de session sont

stockées sur les ordinateurs dans chaque RGT, il n'est pas obligatoire d'utiliser des clés d'installation pour chiffrer ces clés de session.

L'utilisation d'une hiérarchie de clés de chiffrement à deux étages est appelée concept de “hiérarchie de clés”. De surcroît le “concept de séparation de clés” nécessite d'être pris aussi en charge dans les systèmes de gestion de clés privées. La séparation de clés impose que les clés utilisées pour l'authentification ne doivent pas être utilisées pour le contrôle d'accès, pour la confidentialité des données, etc. Par conséquent, les clés pour chaque service de sécurité OSI qui est nécessaire à une application particulière de l'interface X du RGT doivent avoir des procédures distinctes pour la création, le stockage, la distribution, l'utilisation et la suppression. En suivant rigoureusement ce concept, l'utilisateur du RGT peut remédier à une interruption de sécurité et minimiser l'influence totale exercée sur les diverses communications prises en charge à travers l'interface X du RGT.

Pour la transmission de gros volumes de clés par l'interface X du RGT, les clés elles-mêmes doivent être classées dans des fichiers de clés de sécurité. Cela permet l'utilisation du service de transfert de données et des mécanismes de protocole de sécurité décrits dans la Recommandation Q.812. Les deux utilisateurs du RGT doivent fournir régulièrement un fichier de texte chiffré contenant une liste de 1000 clés. Cela permet une alimentation pendant un an. A partir de cet ensemble, l'administrateur du RGT indiquera le membre qui sera la clé valable utilisée pour la prochaine session sur l'interface X du RGT. La clé effective sera sélectionnée de manière aléatoire à des intervalles aléatoires, par un ou par les deux utilisateurs du RGT. Le choix d'une nouvelle clé nécessitera de commencer à un moment accepté par les deux utilisateurs.

Les fichiers de sauvegarde relatifs à la sécurité doivent contenir des indices qui sont des multiples de 10 000 pour des questions de réserve. La convention de dénomination pour les fichiers de sauvegarde relatifs aux clés de sécurité est: keys.networkid.bk, où networkid est le nom d'identification réseau pour l'administration/exploitation reconnue et où bk est le numéro séquentiel du fichier à partir de 10 000. Les fichiers de sauvegarde sont utilisés lorsque:

1) le fichier considéré a été compromis;

2) le fichier considéré a utilisé toutes les clés;

3) le fichier considéré a été altéré.

Une fois qu'un fichier de sauvegarde a été utilisé, l'agent doit fournir un nouveau fichier de sauvegarde avec un nouvel ensemble de clés et d'indices de sauvegarde. Les nouveaux indices commenceront au prochain multiple de 10 000 en séquence.

APPENDICE III

Informations supplémentaires sur le chiffrement de données

Le registre de l'ISO, pour les techniques de chiffrement fournit la plupart des bases pour l'utilisation de la sécurité dans les applications internationales. Le choix ou la sélection d'un algorithme de chiffrement particulier sort largement du cadre de la présente Recommandation et des autres Recommandations de l'UIT sur le RGT. Cependant, deux utilisateurs de RGT peuvent faire appel au registre de l'ISO pour les algorithmes de chiffrement et se mettre d'accord sur celui qui satisfera leurs besoins.

L'ISO 9979 définit les procédures pour l'enregistrement d'informations associé aux algorithmes de chiffrement de la manière suivante:

a) un nom formel d'entrée ISO pour l'algorithme;

b) le nom privé (ou les noms) donné(s) à l'algorithme par son auteur ou par son propriétaire;

c) le domaine d'application prévu pour les algorithmes;

d) les prescriptions d'interface de chiffrement;

e) une série de mots tests pour vérifier la fonctionnalité de base;

f) l'identité de l'organisation qui a demandé l'enregistrement de l'algorithme;

g) les dates de l'enregistrement et des modifications;

h) l'existence éventuelle d'une norme nationale à ce sujet;

i) les restrictions concernant les licences de brevets;

A titre facultatif, le registre de l'ISO pour les algorithmes de chiffrement peut aussi comprendre:

j) une liste de références à tous les algorithmes associés;

k) la description de l'algorithme;

l) les modes opératoires;

m) d'autres informations.

On pourra se reporter à l'ISO 9979 pour de plus amples détails.

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	**Maintenance: 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 Z	Langages de programmation