UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T E.408

(05/2004)

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

SÉRIE E: EXPLOITATION GÉNÉRALE DU RÉSEAU, SERVICE TÉLÉPHONIQUE, EXPLOITATION DES SERVICES ET FACTEURS HUMAINS

Gestion de réseau – Gestion du réseau international

Prescriptions de sécurité des réseaux de télécommunication

Recommandation UIT-T E.408

RECOMMANDATIONS UIT-T DE LA SÉRIE E

EXPLOITATION GÉNÉRALE DU RÉSEAU, SERVICE TÉLÉPHONIQUE, EXPLOITATION DES SERVICES ET FACTEURS HUMAINS

EXPLOITATION DES RELATIONS INTERNATIONALES	
Définitions	E.100–E.103
Dispositions de caractère général concernant les Administrations	E.104–E.119
Dispositions de caractère général concernant les usagers	E.120–E.139
Exploitation des relations téléphoniques internationales	E.140–E.159
Plan de numérotage du service téléphonique international	E.160–E.169
Plan d'acheminement international	E.170–E.179
Tonalités utilisées dans les systèmes nationaux de signalisation	E.180–E.189
Plan de numérotage du service téléphonique international	E.190–E.199
Service mobile maritime et service mobile terrestre public	E.200–E.229
DISPOSITIONS OPÉRATIONNELLES RELATIVES À LA TAXATION ET À LA COMPTABILITÉ DANS LE SERVICE TÉLÉPHONIQUE INTERNATIONAL	
Taxation dans les relations téléphoniques internationales	E.230–E.249
Mesure et enregistrement des durées de conversation aux fins de la comptabilité	E.260–E.269
UTILISATION DU RÉSEAU TÉLÉPHONIQUE INTERNATIONAL POUR LES APPLICATIONS NON TÉLÉPHONIQUES	
Généralités	E.300–E.319
Phototélégraphie	E.320–E.329
DISPOSITIONS DU RNIS CONCERNANT LES USAGERS	E.330–E.349
PLAN D'ACHEMINEMENT INTERNATIONAL	E.350–E.399
GESTION DE RÉSEAU	
Statistiques relatives au service international	E.400–E.404
Gestion du réseau international	**E.405–E.419**
Contrôle de la qualité du service téléphonique international	E.420–E.489
INGÉNIERIE DU TRAFIC	
Mesure et enregistrement du trafic	E.490–E.505
Prévision du trafic	E.506–E.509
Détermination du nombre de circuits en exploitation manuelle	E.510–E.519
Détermination du nombre de circuits en exploitation automatique et semi-automatique	E.520–E.539
Niveau de service	E.540–E.599
Définitions	E.600–E.649
Ingénierie du trafic des réseaux à protocole Internet	E.650–E.699
Ingénierie du trafic RNIS	E.700–E.749
Ingénierie du trafic des réseaux mobiles	E.750–E.799
QUALITÉ DE SERVICE: CONCEPTS, MODÈLES, OBJECTIFS, PLANIFICATION DE LA SÛRETÉ DE FONCTIONNEMENT	
Termes et définitions relatifs à la qualité des services de télécommunication	E.800–E.809
Modèles pour les services de télécommunication	E.810–E.844
Objectifs et concepts de qualité des services de télécommunication	E.845–E.859
Utilisation des objectifs de qualité de service pour la planification des réseaux de télécommunication	E.860–E.879
Collecte et évaluation de données d'exploitation sur la qualité des équipements, des réseaux et des services	E.880–E.899

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

Recommandation UIT-T E.408

Prescriptions de sécurité des réseaux de télécommunication

Résumé

La présente Recommandation donne un aperçu général des prescriptions de sécurité et définit un cadre qui identifie les menaces qui pèsent sur la sécurité des réseaux de télécommunication en général (fixes ou mobiles; voix et données) et indique comment planifier des contre-mesures afin de limiter les risques découlant de ces menaces.

Source

La Recommandation UIT-T E.408 a été approuvée le 28 mai 2004 par la Commission d'études 2 (2001-2004) de l'UIT-T selon la procédure définie dans la Résolution 1 de l'AMNT.

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

Recommandation UIT-T E.408

Prescriptions de sécurité des réseaux de télécommunication

1 Introduction

1.1 Domaine d'application

La présente Recommandation donne un aperçu général et définit un cadre qui identifie les menaces qui pèsent sur la sécurité des réseaux de télécommunication en général (fixes ou mobiles; voix et données) et indique comment planifier des contre-mesures afin de limiter les risques découlant de ces menaces.

Par sa nature, la présente Recommandation a un caractère générique et n'identifie pas ou ne traite pas de prescriptions correspondant à des réseaux particuliers.

La présente Recommandation ne cherche pas non plus à définir des nouveaux services de sécurité mais utilise les services de sécurité existants définis dans d'autres Recommandations UIT-T et dans les normes élaborées par d'autres organismes.

La présente Recommandation est destinée à favoriser la coopération internationale dans les domaines ci-dessous relatifs à la sécurité des réseaux de télécommunication:

- mise en commun et diffusion de l'information;
- coordination en cas d'incident et réponse aux situations de crise;
- recrutement et formation de professionnels de la sécurité;
- coordination de l'application des règlements;
- protection des infrastructures et services critiques;
- élaboration d'une législation appropriée.

Pour faciliter cette coopération, il est essentiel d'appliquer à l'échelle nationale les prescriptions énoncées dans la présente Recommandation en ce qui concerne les composants nationaux du réseau.

1.2 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.

– Recommandation UIT-T M.3010 (2000), *Principes du réseau de gestion des télécommunications*.

– Recommandation UIT-T M.3016 (1998), *Aperçu général de la sécurité du RGT*.

– Recommandation UIT-T M.3400 (2000), *Fonctions de gestion du réseau de gestion des télécommunications*.

– Recommandation UIT-T X.509 (2000) | ISO/CEI 9594-8:2001, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre général des certificats de clé publique et d'attribut*.

– Recommandation UIT-T X.741 (1995) | ISO/CEI 10164-9:1995, *Technologies de l'information – Interconnexion des systèmes ouverts – Gestion-systèmes: Objets et attributs pour le contrôle d'accès*.

– Recommandation UIT-T X.800 (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT*.

– Recommandation UIT-T X.802 (1995) | ISO/CEI TR 13594:1995, *Technologies de l'information – Modèle de sécurité des couches inférieures*.

– Recommandation UIT-T X.803 (1994) | ISO/CEI 10745:1995, *Technologies de l'information – Interconnexion des systèmes ouverts – Modèle de sécurité pour les couches supérieures*.

– Recommandation UIT-T X.805 (2003), *Architecture de sécurité pour les systèmes assurant des communications de bout en bout*.

– Recommandation UIT-T X.810 (1995) | ISO/CEI 10181-1:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: aperçu général*.

– Recommandation UIT-T X.812 (1995) | ISO/CEI 10181-3:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: cadre de contrôle d'accès*.

– Recommandation UIT-T X.813 (1996) | ISO/CEI 10181-4:1997, *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: non-répudiation*.

– Recommandation UIT-T X.814 (1995) | ISO/CEI 10181-5:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: cadre de confidentialité*.

– Recommandation UIT-T X.815 (1995) | ISO/CEI 10181-6:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: cadre d'intégrité*.

– Recommandation UIT-T X.816 (1995) | ISO/CEI 10181-7:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: cadre d'audit et d'alarmes de sécurité*.

– ISO/CEI 9979:1999, *Technologies de l'information – Techniques de sécurité – Procédures d'enregistrement des algorithmes cryptographiques*.

– IETF RFC 2535 (1999), *Domain Name System Security Extensions*.

– IETF RFC 2870 (2000), *Root Name Server Operational Requirements*.

– IETF RFC 3013 (2000), *Recommended Internet Service Provider Security Services and Procedures*.

1.3 Utilisation du terme service

Tel qu'il est employé dans la présente Recommandation, le terme service ne désigne aucun des services définis par l'UIT. Il s'agit en revanche d'un terme générique employé à propos des aspects et/ou des fonctions de sécurité examinés et il faudra le définir dans l'avenir.

1.4 Justification

La demande visant à disposer d'un cadre générique concernant la sécurité des réseaux de télécommunications internationales émane de plusieurs entités:

– **les clients/abonnés** qui ont besoin d'avoir confiance dans le réseau et les services offerts, et qui souhaitent que les services (en particulier les services d'urgence) soient disponibles en cas de catastrophe majeure, y compris les actions terroristes;

– **la communauté/l'autorité publique** qui exige une sécurité définie par des directives et des lois, garantissant la disponibilité des services, l'existence d'une concurrence loyale et la protection de la confidentialité;

– l**es opérateurs de réseau et les fournisseurs de services** qui eux aussi ont besoin de sécurité pour sauvegarder leurs activités et leurs intérêts et remplir leurs obligations vis-à-vis des clients et du public, tant au niveau national qu'au niveau international.

Les prescriptions de sécurité des réseaux de télécommunication devraient être de préférence fondées sur des normes internationales de sécurité déjà admises car il est préférable d'en réutiliser que d'en créer de nouvelles. La fourniture et l'utilisation de services et mécanismes de sécurité peuvent être assez coûteuses comparées à la valeur des transactions à protéger. Il est par conséquent important de pouvoir personnaliser la sécurité assurée afin qu'elle soit en rapport avec les services à protéger. Les services et mécanismes de sécurité qui sont utilisés doivent permettre leur personnalisation. En raison du très grand nombre de combinaisons possibles de caractéristiques de sécurité, il est souhaitable de disposer de **profils de sécurité** (voir Appendice II) qui couvrent un vaste éventail de services de réseau de télécommunication.

La normalisation facilitera la **réutilisation de solutions et de produits** et permettra ainsi une mise en œuvre plus rapide et moins coûteuse de mesures de sécurité.

Pour les fournisseurs et les utilisateurs de systèmes, les principaux avantages des solutions normalisées sont l'économie d'échelle dans l'élaboration des produits et l'interopérabilité des composants des réseaux de télécommunication pour ce qui est de la sécurité.

Il est nécessaire d'assurer des services et d'offrir des mécanismes de sécurité pour protéger les réseaux de télécommunication contre les attaques malveillantes tels les refus de service, les écoutes indiscrètes, l'usurpation d'identité, la réorganisation de messages (modification, retard, suppression, insertion, reproduction, réacheminement, mauvais acheminement ou réorganisation des messages), la répudiation ou la falsification. La protection fait intervenir la prévention, la détection et le rétablissement après attaque, ainsi que la gestion des informations concernant la sécurité. La protection doit également inclure des mesures visant à empêcher des interruptions de service dues à des évènements naturels (météorologie, etc.) ou à des attaques malveillantes (actions terroristes). Les dispositions doivent être prises pour permettre l'écoute et la surveillance lorsque celles-ci sont dûment autorisées par les autorités judiciaires.

2 Description du système

Pour sécuriser efficacement un réseau, il est recommandé d'implémenter des couches de sécurité – la sécurité sera d'autant plus grande que le nombre de couches sera grand. Cette technique de structuration en couches peut être analysée de bas en haut comme suit:

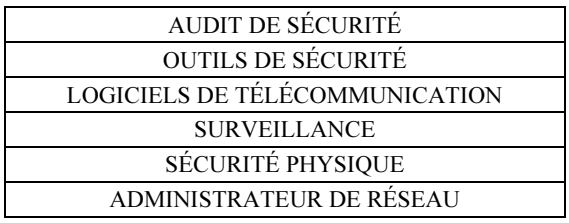

Figure 1/E.408 – Structuration en six couches de la sécurité de réseau

Dans la présente Recommandation, le terme "couche" sert simplement à décrire certaines considérations relatives à la sécurité afin d'organiser la sécurité des réseaux. Les différentes couches décrites dans la présente Recommandation ne doivent pas être considérées comme des éléments architecturaux et elles ne doivent pas être confondues avec les couches de sécurité de la Rec. UIT-T X.805.

Tout comme les fondations d'un immeuble, la première couche – administrateur de réseau – sera l'élément organisationnel le plus important de la sécurité du réseau. Affecter des crédits annuels supplémentaires pour avoir un bon administrateur de réseau est mille fois plus judicieux que d'acheter un pare-feu coûteux. Les bons administrateurs de réseau connaissent parfaitement les systèmes d'exploitation sur lesquels ils travaillent et savent comment verrouiller chaque machine de leur réseau pour limiter uniquement l'accès aux ports et aux processus nécessaires. Les responsables doivent faire en sorte que les administrateurs de réseau bénéficient d'une formation en permanence et disposent du temps nécessaire pour se tenir informés des bogues et des abus qui affectent les réseaux.

La deuxième couche est la couche sécurité physique. Tout attaquant sait que la façon la plus aisée d'accéder à un réseau est de le faire depuis l'intérieur. Il y a même de très nombreux cas d'espionnage relationnel ("social engineering") dans lesquels les attaquants ont simplement appelé le service client et indiqué qu'ils avaient oublié leur mot de passe et demandaient au service client de bien vouloir le changer en xxxxx. La sécurité physique inclut de très nombreuses mesures allant de la limitation de l'accès aux consoles à certaines personnes (administrateurs de systèmes) à des politiques définissant les informations non confidentielles concernant le réseau. Les choix politiques appropriés en matière d'utilisation de mot de passe et d'installation de logiciel aident beaucoup à limiter l'accès au réseau.

La troisième couche est la couche surveillance. Il est très rare qu'une attaque soit couronnée de succès dès le premier essai. La plupart des attaques pourraient être stoppées si l'on consultait seulement une fois par jour le fichier/journal système. Cela ne prend pas autant de temps qu'il y paraît. Il n'y a pas de meilleur dispositif d'analyse des fichiers journaux que l'œil humain. Il existe plusieurs bons logiciels qui permettent de suivre les fichiers journaux; malgré la très grande utilité de ces programmes, l'administrateur système doit lire le fichier/journal de ses principales machines chaque jour.

La quatrième couche est la couche logiciels de télécommunication. Chaque élément de logiciel placé sur des serveurs doit être évalué en ne perdant pas de vue la sécurité. L'administrateur système doit savoir, par exemple, quel port TCP et UDP le logiciel observera, avec quelconque utilisateur le logiciel interagira et les autorisations d'annuaire que le logiciel requiert. Il est également recommandé d'analyser avant l'achat les bogues concernant la sécurité déjà connus. Cela doit faire partie du processus d'évaluation de tous les logiciels que l'on veut acheter.

La cinquième couche est la couche outils de sécurité. Après avoir mis en place de bonnes politiques et pratiques pour les quatre couches précédentes, il est nécessaire de s'intéresser aux pare-feu, aux logiciels de détection d'intrusion et aux mandats. Installer les meilleurs pare-feu du monde associés à de mauvaises politiques de pare-feu est pire que de ne pas avoir de pare-feu du tout. Bien trop souvent, on trouve des serveurs de réseau dont la politique de sécurité ne repose que sur des pare-feu. Une fois le pare-feu franchi, tous les serveurs deviennent largement ouverts aux attaques.

La sixième couche est la couche audit de sécurité. La sécurité de réseau est un objectif évolutif. Tous les jours, quelqu'un, quelque part, trouve un nouveau moyen d'attaque. Il est important de tenter régulièrement de pénétrer dans son propre réseau. Dans un audit, on doit tester chaque aspect de la sécurité du réseau. Il est recommandé de tester la sécurité physique vis-à-vis des attaques et de disposer d'une personne pouvant exécuter un programme "war dialer" sur tous les numéros de téléphone pour s'assurer que personne n'a installé un modem sur un ordinateur sans que l'administrateur de réseau en ait eu connaissance. Les audits doivent être effectués sur les serveurs de courrier électronique, les serveurs de noms de domaine, les domaines, le Web et les serveurs FTP.

2.1 Les différents acteurs et leurs rôles

Dans le cadre de la normalisation des réseaux de télécommunication, on ne s'intéressera qu'à la sécurité technique, ce qui signifie que les acteurs concernés sont des *acteurs de télécommunication.* Un acteur de télécommunication est une personne (physique ou morale) ou un processus qui a la charge de certaines opérations du réseau.

Chaque fois qu'un acteur de télécommunication exécute une action, il assume un rôle. Dans certains cas, il y aura une relation univoque entre un acteur de télécommunication et un rôle, c'est-à-dire que l'acteur assumera toujours dans le même rôle. Dans d'autres cas, il y aura une relation de un à plusieurs entre un utilisateur acteur de télécommunication particulier et les rôles qu'il peut assumer.

On trouvera ci-après un classement de certains rôles courants:

– opérateurs de réseau (*public ou privé*);
– fournisseurs de services (*fournisseurs de services support ou fournisseurs de services à valeur ajoutée*);
– abonnés au service/client du service;
– utilisateurs finaux du service;
– fournisseurs d'équipement/de logiciel;
– tierce partie de confiance.

2.2 Domaines de sécurité des réseaux de télécommunication

Un *domaine de sécurité* est défini comme un ensemble d'entités et de protagonistes soumis à une seule politique de sécurité et à une seule administration de la sécurité.

Pour la conception de la sécurité de réseau on peut prendre en compte différents domaines et sous-domaines pour cerner et délimiter les responsabilités en matière de gestion de réseau et de contrôle de la sécurité.

Au minimum, les aspects suivants doivent être pris en compte pour la subdivision du réseau en domaines:

• les limites physiques du réseau;
• les domaines de responsabilité;
• les champs des fonctionnalités;
• le caractère critique des applications et des données circulant dans les réseaux;
• les limites géographiques potentielles (bâtiments, habitudes régionales, etc.);
• les besoins/disponibilités en trafic et en capacité;
• les besoins de continuité et de rétablissement;
• le domaine d'application d'entreprise;
• le domaine d'appui à l'entreprise (facturation, gestion des ressources humaines, etc.);

- les domaines de développement et de test;
- les domaines de production;
- le domaine de gestion des alarmes;
- les responsabilités de gestion et d'administration de la sécurité des réseaux.

Les interfaces de couche d'infrastructure sont typiques d'une zone où les responsabilités changent. L'interface entre un environnement de production et un environnement de bureau, ou l'environnement de test, sont des limites type de fonctionnalité du réseau. Chaque point d'accès à un domaine ou à un sous-domaine nécessite une passerelle, qui peut offrir plusieurs services de sécurité tels la gestion du trafic, le contrôle d'accès, etc.

3 Objectifs génériques de sécurité pour les réseaux de télécommunication

L'objet du présent paragraphe est de décrire le but ultime des mesures de sécurité prises dans les réseaux de télécommunication. L'accent est mis sur les prescriptions de sécurité qui sont satisfaites et non pas sur la façon dont elles sont mises en œuvre.

Les objectifs en matière de sécurité pour les réseaux de télécommunication sont les suivants:

– seuls les acteurs légitimes devraient pouvoir accéder et utiliser les réseaux de télécommunication;

– les acteurs légitimes devraient pouvoir accéder et opérer sur les ressources pour lesquelles ils disposent d'autorisations d'accès;

– les réseaux de télécommunication devraient offrir le niveau de confidentialité fixé par les politiques de sécurité qui leur sont applicables;

– tous les acteurs devraient être tenus responsables de leurs actions et uniquement de leurs actions dans les réseaux de télécommunication;

– afin d'en garantir la disponibilité, les réseaux de télécommunication devraient être protégés contre des accès ou des opérations non sollicités;

– il devrait être possible de retrouver les informations relatives à la sécurité depuis les réseaux de télécommunication (mais seuls les acteurs légitimes devraient pouvoir retrouver ces informations);

– lorsque des violations de la sécurité sont détectées, celles-ci devraient être gérées de façon contrôlée conformément à un plan prédéfini de manière à minimiser les dommages potentiels;

– en cas de détection d'une atteinte à la sécurité, il devrait être possible de rétablir les niveaux de sécurité normaux;

– l'architecture en matière de sécurité des réseaux de télécommunication devrait offrir une certaine souplesse afin de prendre en charge différentes politiques de sécurité, par exemple des robustesses différentes des mécanismes de sécurité.

L'expression "accéder à des ressources" est entendue non seulement comme la possibilité d'exécuter des fonctions mais également de lire des informations.

Les objectifs génériques sont énoncés conformément au point de vue et à la sémantique utilisée dans la gestion de l'entreprise. Les paragraphes qui suivent sont exprimés en termes plus techniques conduisant à des services et des fonctions de sécurité susceptibles d'être implémentés. Le mappage entre les deux langages n'est pas toujours évident.

On peut montrer qu'en remplissant l'ensemble suivant d'objectifs de sécurité, les cinq premiers objectifs de sécurité précités pour les réseaux de télécommunication dans le présent paragraphe seront remplis, à savoir:

– la confidentialité;

– l'intégrité des données (l'intégrité des programmes système est certainement aussi requise ou sinon avez-vous eu une attaque du DoS?);
– la responsabilité, y compris l'authentification, la non-répudiation et le contrôle d'accès;
– la disponibilité.

Les menaces et les risques identifiés au § 5 et les prescriptions fonctionnelles définies au § 6 seront exprimés avec ces termes plus formels. On se reportera au § 5 pour les définitions.

Des objectifs restants portent sur la surveillance et le contrôle de l'état de sécurité du système. Ces objectifs seront traités dans les paragraphes consacrés à la récupération, l'architecture et la gestion de la sécurité conformément à la politique de sécurité implémentée.

4 Questions juridiques

L'infrastructure de sécurité d'un réseau de télécommunication doit pouvoir prendre en charge les contraintes imposées par les lois, la législation contractuelle, les traités et la réglementation. Parmi ces contraintes on peut citer par exemple les services de sécurité obligatoires (tels que garantir la confidentialité de l'information client), l'exclusion de certains mécanismes de sécurité (tels certains types de chiffrement) et/ou les écoutes faites par des organismes légaux.

5 Menaces et risques

Le présent paragraphe a pour objet d'explorer les menaces et les risques qui pèsent sur les réseaux de télécommunication. Il ne s'agit pas d'évaluer les risques ou d'analyser les menaces pour des types particuliers de télécommunication qui sont des questions locales pouvant être traitées différemment par chaque opérateur sans affecter l'interopérabilité.

Une menace est une violation potentielle de la sécurité. Selon les objectifs génériques de sécurité identifiés, les menaces peuvent être dirigées sur quatre types d'objectifs différents à savoir:

– **la confidentialité** (la confidentialité de l'information stockée et transférée);
– **l'intégrité des données** (protection des informations stockées et transférées);
– **l'intégrité du système** (protection du système d'exploitation);
– **la responsabilité** (toute entité doit être responsable des actions qu'elle a déclenchées);
– **la disponibilité** (toutes les entités autorisées doivent avoir un accès correct aux réseaux de télécommunication).

Dans la présente Recommandation, on distingue trois types de menaces:

– la menace accidentelle: une menace dont l'origine n'est pas consécutive à une malveillance;
– la menace administrative: une menace qui découle d'un manque d'administration de la sécurité;
– la menace intentionnelle: une menace qui fait intervenir une entité malveillante qui peut attaquer les échanges par réseau de télécommunication ou les ressources de réseau.

Dans les travaux de normalisation, il peut être tenu compte des menaces accidentelles et administratives pour autant que leurs conséquences soient les mêmes que les menaces intentionnelles. Afin de procéder à une analyse plus précise des menaces, la présente Recommandation met l'accent sur les menaces intentionnelles. L'objet de cette approche est de fournir une liste brève des menaces dont il peut être tenu directement compte dans les travaux de normalisation. Une analyse des menaces doit ainsi concerner les points suivants fondés sur la Rec. UIT-T X.800:

– **usurpation d'identité**: prétention qu'a une entité d'en être une autre;

– **écoute illicite**: violation de la confidentialité par écoute des échanges par réseau de télécommunication;

– **accès non autorisé**: tentative d'une entité d'accéder à des données en violation de la politique de sécurité en vigueur;

– **perte ou altération des informations**: l'intégrité des données transférées est compromise par une suppression, une insertion, une modification, une réorganisation, une relecture ou l'ajout d'un retard et ce, de façon non autorisée;

– **répudiation**: le fait pour des entités impliquées dans des échanges par réseau de télécommunication de nier par la suite avoir participé à ces échanges;

– **falsification**: une entité élabore une information et déclare que cette information a été reçue en provenance d'une autre entité ou envoyée à une autre entité;

– **refus de service**: phénomène qui se produit lorsqu'une entité ne parvient pas à exécuter ses fonctions ou empêche d'autres entités d'exécuter leurs fonctions. Cela peut inclure le refus d'accès aux réseaux de télécommunication et le refus d'échange par réseau de télécommunication en inondant les réseaux ou les composantes d'un réseau. Dans un réseau partagé, cette menace peut être reconnue comme étant la création d'un trafic supplémentaire qui vient inonder le réseau, les utilisateurs étant ainsi empêchés d'utiliser le réseau car leur trafic est retardé.

Le Tableau 1 donne le mappage entre les menaces et les objectifs.

Tableau 1/E.408 – Mappage entre menaces et objectifs

Menaces	Objectifs			
	Confidentialité	**Intégrité du système ou des données**	**Responsabilité**	**Disponibilité**
Usurpation d'identité	x	x	x	x
Ecoutes illicites	x			
Accès non autorisé	x	x	x	x
Perte ou altération de l'information (transférée)		x		x
Répudiation			x	
Falsification		x	x	
Refus de service				x

Une menace potentielle qui peut peser sur un système est en principe sans conséquence sauf s'il existe une faiblesse correspondante dans le système et un moment où cette faiblesse peut être exploitée. Chaque menace implique un risque. L'évaluation du risque peut être subdivisée en deux à savoir l'évaluation de probabilité de chaque menace et l'évaluation de l'impact que cette menace peut avoir. L'évaluation de la menace et du risque doit faire partie d'un processus itératif: de nouvelles menaces peuvent apparaître lorsque des contre-mesures sont mises en place, par exemple des menaces concernant les clés cryptographiques lorsque des mesures de type cryptographique ont été mises en place.

6 Prescriptions de sécurité

La Figure 2 décrit les relations entre les objectifs de sécurité, les menaces, les risques, les prescriptions de sécurité et les services. Elle décrit le processus qui permet de déterminer les prescriptions de sécurité à partir des menaces et des objectifs de sécurité qui à leur tour seront

satisfaits par un ensemble de services de sécurité. Ces services, qui pallient les menaces, utiliseront des mécanismes qui eux-mêmes utiliseront des algorithmes de sécurité.

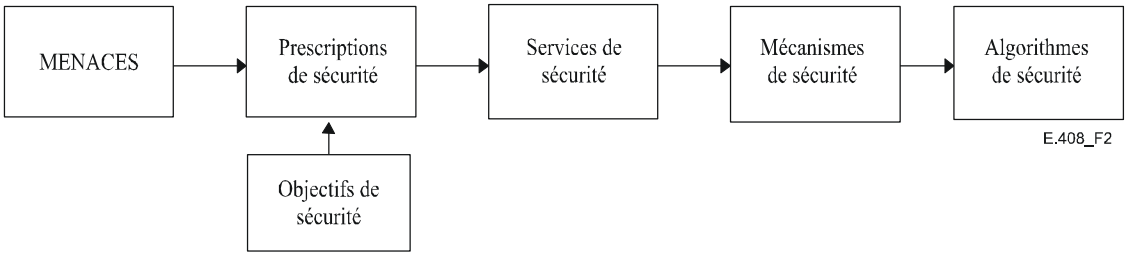

Figure 2/E.408 – Prescriptions de sécurité

Le paragraphe 6.1 donne la liste des prescriptions de sécurité. Sauf indication contraire, le terme "prescription" utilisé dans cette Recommandation ne signifie pas que la présence d'une certaine fonctionnalité est toujours obligatoire dans chaque réseau de télécommunication; en revanche, il signifie qu'une fonctionnalité peut être rendue obligatoire par un administrateur de réseau pour certains services, applications et/ou interfaces spécifiques de ce réseau. Le choix réel dépendra des objectifs de sécurité énoncés dans la politique de sécurité de l'opérateur.

Outre les prescriptions de sécurité et les services, le présent paragraphe décrit également certaines prescriptions génériques pour la gestion des services de sécurité (voir § 6.2) et des prescriptions architecturales gouvernant l'intégration des services de sécurité dans une architecture générique de réseau (voir § 6.3). Les prescriptions administratives et de durée de vie sont importantes mais n'affecteront pas l'architecture et sortent donc du cadre du présent paragraphe.

Les prescriptions de sécurité peuvent être appliquées à chaque perspective de sécurité de l'architecture de sécurité normalisée dans la Rec. UIT-T X.805. Les dimensions de sécurité (également définies dans la Rec. UIT-T X.805) sont conçues pour satisfaire aux prescriptions de sécurité pour chaque perspective de sécurité. Les services de sécurité, les mécanismes de sécurité et les algorithmes de sécurité examinés dans la présente Recommandation doivent être considérés comme faisant partie intégrante de chaque dimension de sécurité.

6.1 Prescriptions de sécurité et services correspondants

Le présent paragraphe décrit un ensemble de prescriptions fonctionnelles génériques et les services correspondants qui peuvent être utilisés pour pallier les menaces qui visent les réseaux de télécommunication.

6.1.1 Mappage entre prescriptions fonctionnelles, menaces et objectifs de sécurité

Le présent paragraphe identifie les prescriptions fonctionnelles de sécurité couvrant les menaces dont la liste est donnée dans le § 5, c'est ce qu'illustre le Tableau 2. A partir de cela, les prescriptions de sécurité ont été mappées (Tableau 3) avec les objectifs de sécurité énoncés au § 3. La liste est limitée aux prescriptions qui sont génériques par nature et qui ont un important impact sur les diverses composantes et l'architecture.

Tableau 2/E.408 – Mappage entre prescriptions fonctionnelles et menaces

Prescriptions fonctionnelles	Menaces						
	Usurpation d'identité	Ecoutes illicites	Accès non autorisé	Perte ou altération des informations	Répu-diation	Falsifi-cation	Refus de service
Vérification des identités	x		x				
Accès contrôlé et autorisation			x				x
Protection de la confidentialité		x	x				
Protection de l'intégrité des données				x			
Responsabilité					x	x	
Consignation des activités	x		x		x	x	x
Signalisation des alarmes	x		x	x			x
Audit	x		x		x	x	x

Les objectifs retenus sont les quatre objectifs génériques définis au § 3, et qui figurent dans les colonnes du Tableau 3, indiquant l'ensemble des prescriptions fonctionnelles auxquelles il faut répondre pour remplir l'objectif en question.

6.1.2 Description des prescriptions fonctionnelles et fonctions correspondantes

Les prescriptions fonctionnelles indiquées dans les Tableaux 2 et 3 sont examinées plus avant ci-après et, pour chacune des prescriptions, les fonctions correspondantes sont identifiées. Il est à noter que les prescriptions, pour ces fonctions, n'entraînent pas automatiquement la mise en place d'un service de sécurité tel que défini par l'ISO. Dans la pratique toutefois, il y a coïncidence dans certains cas.

Tableau 3/E.408 – Mappage entre objectifs de sécurité et prescriptions fonctionnelles

Prescriptions fonctionnelles	Objectifs de securité			
	Confidentialité	Intégrité du système ou des données	Responsabilité	Disponibilité
Vérification des identités	x	x	x	
Accès contrôlé et autorisation	x	x	x	x
Protection de la confidentialité	x	x		
Protection du système ou de l'intégrité des données		x		
Responsabilité			x	
Consignation des activités			x	x
Signalisation des alarmes	x	x	x	x
Audit			x	x

NOTE – Le maintien de la confidentialité des données est une condition suffisante pour le maintien de l'intégrité des données, c'est-à-dire que si l'on maintient la confidentialité des données, ces données sont également protégées contre les altérations. Néanmoins, la protection contre les altérations des données ne confère pas nécessairement une protection contre leur divulgation.

6.1.2.1 Vérification des identités

Un réseau de télécommunication doit disposer de capacités permettant d'établir et de vérifier l'identité déclarée de tout acteur dans le réseau de télécommunication.

Des acteurs peuvent être des êtres humains ou des entités à l'intérieur du réseau de télécommunication. Les identités vérifiées constituent la base de la responsabilisation et sont fondamentales pour répondre à la plupart des prescriptions de sécurité dont la liste est donnée dans le présent paragraphe.

Le service de sécurité permettant de prendre en charge cette prescription est l'**authentification**. La fonction d'authentification fournit la preuve que l'identité d'un objet ou d'un sujet correspond à l'identité que cet objet ou ce sujet déclare avoir. Selon le type d'acteur et pour les besoins de l'identification, il peut être nécessaire de disposer des types suivants d'authentification, à savoir:

– l'authentification de l'utilisateur établissant la preuve de l'identité de l'utilisateur humain ou du processus d'application;
– l'authentification de l'entité homologue, établissant la preuve de l'identité de l'entité homologue pendant un échange par réseau de télécommunication;
– l'authentification de l'origine des données, établissant la preuve de l'identité responsable d'une unité de données particulière.

L'utilisation de la fonction d'authentification permet d'établir la preuve pendant une instance particulière de temps. Pour garantir une preuve permanente, l'authentification doit être répétée ou liée à un service d'intégrité.

Parmi les mécanismes utilisés pour implémenter un service d'authentification, citons les mots de passe et les numéros d'identification personnels (PIN, *personal identification number*) (authentification simple) et les méthodes cryptographiques (authentification forte).

6.1.2.2 Accès contrôlé et autorisation

Un réseau de télécommunication peut disposer de capacités empêchant les acteurs d'avoir accès à des informations ou à des ressources auxquelles ils ne sont pas autorisés à avoir accès.

Le service de sécurité permettant de répondre à cette prescription est le **contrôle d'accès**. Le service de contrôle d'accès fournit un moyen garantissant que seules les personnes autorisées ont accès aux ressources. Les ressources concernées peuvent être le système physique, le logiciel système, les applications et les données. La fonction de contrôle d'accès peut être définie et mise en œuvre à différents niveaux de granularité dans un réseau de télécommunication, à savoir: au niveau de l'agent, au niveau des objectifs ou au niveau des attributs. Les restrictions d'accès sont consignées dans l'information de contrôle d'accès qui spécifie:

– le moyen de déterminer quelles entités sont autorisées à avoir accès;
– le type d'accès autorisé (lecture, écriture, modification, création, suppression).

Plus spécifiquement, le contrôle d'accès du réseau de télécommunication peut être scindé en trois types:

– *Le contrôle d'accès au niveau de l'association de gestion*

  Permet le contrôle d'accès au niveau de l'association de gestion, ce qui signifie que les droits d'accès sont liés à l'association elle-même, autrement dit, il s'agit du droit d'établir l'association.

– *Le contrôle d'accès aux notifications de gestion*

  Permet le contrôle d'accès aux notifications, autrement dit ce contrôle garantit que les notifications ne sont divulguées qu'aux entités habilitées à les recevoir.

– *Le contrôle d'accès aux ressources gérées*

  Assure le contrôle d'accès aux ressources elles-mêmes.

L'identité de l'entité qui essaie d'avoir accès doit être vérifiée avant d'autoriser l'accès à la ressource. Cela signifie que l'utilisation du contrôle d'accès est toujours liée à l'utilisation de la fonction d'authentification.

6.1.2.3 Protection de la confidentialité

Un réseau de télécommunication doit disposer de capacités garantissant la confidentialité des données stockées et des données communiquées.

Les services de sécurité permettant de prendre en charge cette prescription sont: le **contrôle d'accès** pour les systèmes, le **contrôle d'accès** pour les données stockées et la **confidentialité des données** acheminées par réseau de télécommunication.

La violation de la confidentialité du système ne doit pas être sous-estimée étant donné qu'elle précède généralement des attaques visant le système ou l'intégrité des données (aide les attaquants à trouver les vulnérabilités de type DoS).

Le service de confidentialité assure la protection contre la divulgation non autorisée des données stockées ou échangées. On distingue les types suivants de confidentialité:

– confidentialité du système (inclut des informations aussi diverses que des informations architecturales ou de configuration, les algorithmes utilisés, les numéros de version des logiciels, les types de matériel utilisés, etc.);
– confidentialité sélective d'un domaine;
– confidentialité des connexions;
– confidentialité des flux de données.

6.1.2.4 Protection du système et intégrité des données

Un réseau de télécommunication doit être en mesure de garantir l'intégrité des systèmes et des données stockées ou communiquées.

Les services de sécurité permettant la prise en charge de cette prescription sont: le **contrôle d'accès** aux systèmes, le **contrôle d'accès** aux données stockées et l'**intégrité des données** pour les données communiquées.

Le service d'intégrité permet de garantir l'exactitude des fichiers système et des données échangées, les protégeant contre les modifications, suppressions, créations (insertions) et la lecture des données échangées. On distingue les types suivants d'intégrité:

– intégrité du système d'exploitation;
– intégrité sélective des champs;
– intégrité des connexions sans rétablissement;
– intégrité des connexions avec rétablissement.

6.1.2.5 Responsabilité

Un réseau de télécommunication doit avoir une capacité permettant d'empêcher à une entité donnée de refuser la responsabilité de toutes les actions qu'elle a exécutées ainsi que de leurs effets. Par exemple, un réseau de télécommunication doit avoir les moyens de prouver qu'une entité a exécuté certaines actions.

Cette prescription est prise en charge par le service de **non-répudiation** liant l'individu (ou l'entité) à l'opération exécutée. Les services de non-répudiation sont le moyen de prouver que l'échange de données a vraiment eu lieu et que les utilisateurs connaissent l'environnement légal qui entoure l'utilisation du service ou du produit (par exemple, connaissance que l'utilisation fait l'objet d'une surveillance, etc., ce qu'offre en général le recours à des fanions d'entrée dans le système). Cela apparaît sous trois formes, à savoir:

– la non-répudiation: preuve de l'origine;

– la non-répudiation: preuve de la remise;

– la non-répudiation: preuve de la connaissance de l'environnement légal.

Une façon plus générale, et éventuellement moins contraignante, d'obtention de la responsabilité est le recours à des combinaisons appropriées des services d'**authentification**, de **contrôle d'accès** et de **suivi d'audit**.

6.1.2.6 Consignation des activités, signalement d'alarme et audit

Ces prescriptions répondent à la nécessité de stocker et d'analyser l'information relative aux activités touchant à la sécurité dans le réseau de télécommunication. Les services appropriés sont la **consignation des activités**, le **suivi d'audit** et le **signalement d'alarme**. Chacune de ces conditions est étudiée plus en détail dans ce qui suit.

6.1.2.6.1 Consignation des activités

Un réseau de télécommunication doit disposer de la capacité de stockage des informations concernant les activités du système avec la possibilité de relier cette information à des individus ou à des entités.

Un journal est un organe de stockage des enregistrements: il s'agit de l'abstraction OSI des ressources de consignation dans les systèmes ouverts réels. Les enregistrements contiennent l'information consignée.

Pour les besoins de nombreuses fonctions de gestion, il est nécessaire d'être en mesure de protéger l'information contre des évènements qui se sont produits ou des opérations qui ont été exécutées ou tentées par – ou sur – diverses ressources.

De plus, lorsque cette information est extraite d'un journal, le gestionnaire doit être en mesure de déterminer si des enregistrements ont été perdus ou si les caractéristiques des enregistrements figurant dans le journal ont été modifiées.

Etant donné que les fichiers constituent une partie des données système, cette prescription fait aussi intervenir les prescriptions énoncées au § 6.1.2.4 et peut-être au § 6.1.2.3.

6.1.2.6.2 Signalement des alarmes de sécurité

Un réseau de télécommunication doit disposer de la capacité de générer des notifications d'alarme sur des évènements sélectionnés. L'utilisateur doit être en mesure de définir les critères de sélection.

La fonction contrôle d'audit de sécurité est une fonction de gestion des systèmes qui décrit la notification concernant la collecte des évènements de sécurité. La notification d'alarme de sécurité définie par cette fonction de gestion des systèmes fournit les informations concernant l'état opérationnel touchant à la sécurité.

6.1.2.6.3 Audit de sécurité

Un réseau de télécommunication doit disposer de la capacité d'analyser les données consignées relatives aux évènements de sécurité afin de les utiliser pour contrôler s'il n'y a pas eu violation de la politique de sécurité.

Un audit doit être vu comme une analyse et un examen indépendants des enregistrements et activités du système afin de s'assurer de l'adéquation des commandes de système, pour assurer la conformité avec la politique de sécurité et les procédures opérationnelles établies et détecter les violations des systèmes de sécurité. Le résultat de l'audit permettrait l'identification des modifications qui ont affecté le contrôle, la politique et les procédures.

Le Tableau 4 donne un aperçu général de la relation entre les prescriptions de sécurité et les services de sécurité. Le présent paragraphe définit uniquement les services de sécurité qui font l'objet de solutions normalisées; les autres services envisageables (détection de refus de service ou autres) ne sont pas abordés.

Tableau 4/E.408 – Mappage entre les prescriptions de sécurité et les services de sécurité

Prescription fonctionnelle	Service de sécurité
Vérification des identités	Authentification de l'utilisateur Authentification de l'entité homologue Authentification de l'origine des données
Accès contrôlé et autorisation	Contrôle d'accès
Protection de l'intégrité du système	Contrôle d'accès
Protection de la confidentialité – données stockées	Contrôle d'accès
Protection de la confidentialité – données transférées	Confidentialité
Protection de l'intégrité des données – données stockées	Contrôle d'accès
Protection de l'intégrité des données – données transférées	Intégrité
Responsabilité	Non-répudiation
Consignation de l'activité	Suivi d'audit
Signalement des alarmes de sécurité	Alarme de sécurité
Audit de sécurité	Suivi d'audit et rétablissement

NOTE – Les prescriptions suivantes ne sont pas du même type que celles exprimées précédemment dans le Tableau 4 et peuvent ne pas être vues comme des prescriptions évidentes devant faire l'objet d'une Recommandation. Néanmoins, elles doivent être prises en considération pendant la phase de conception parallèlement à l'implémentation des principales prescriptions de sécurité exprimées plus haut.

6.1.2.6.4 Intégrité du système

Il est essentiel que l'environnement logiciel et matériel des fonctions de sécurité implémentées maintienne le niveau de sécurité requis.

Cela inclut la configuration correcte des systèmes d'exploitation et l'élimination des défauts du système.

Ces aspects ne font pas partie du profil de sécurité fonctionnel lui-même mais ils doivent être énoncés avec ces spécifications afin de garantir la robustesse des fonctions dans l'environnement temps réel.

6.1.2.6.5 Remarques sur la disponibilité

Une prescription concernant la disponibilité n'implique pas la présence d'un seul ou d'un ensemble limité de services de sécurité capables de répondre à cette prescription. Tous les services de sécurité dont la liste est donnée ici devraient former un ensemble cohérent qui, dans sa totalité, est en mesure de maintenir la disponibilité. Les services de sécurité seuls, toutefois, ne seront pas en

mesure de garantir la disponibilité: cela aussi concerne la fiabilité des matériels et des logiciels (du point de vue de la conception de la mise en œuvre).

6.2 Prescriptions concernant la gestion de la sécurité

Un réseau de télécommunication doit contenir des modèles d'information et être doté des capacités de gestion pour les services utilisés pour sécuriser le réseau de télécommunication.

Les prescriptions détaillées concernant la gestion de la sécurité sont l'énoncé des applications de gestion qui devraient être mises en place et de la façon de les concevoir. Cela permet au gestionnaire de la sécurité de disposer des outils appropriés pour surveiller et contrôler les services de sécurité de façon efficace et correcte. Les objectifs de gestion de la sécurité sont présentés à trois niveaux différents du système de télécommunication, qui correspondent à la gestion de la sécurité des systèmes, aux services de sécurité et aux mécanismes de sécurité.

Le rétablissement en un état sécurisé du système après atteinte à la sécurité doit être assuré.

Chaque fois qu'une atteinte à la sécurité se produit, un réseau de télécommunication doit être en mesure de faire face à cette tentative de manière gérée, c'est-à-dire que la tentative ne doit pas se traduire par une dégradation sévère d'un réseau de télécommunication en termes de disponibilité.

Les opérations et les informations relatives à la gestion des services de sécurité dans un réseau de télécommunication nécessitent une attention particulière d'un point de vue de la sécurité. Les clés de cryptage secrètes, l'information d'authentification et les listes de contrôle d'accès sont des exemples où la puissance requise de la protection peut être supérieure à celle correspondant à la gestion de réseau.

6.3 Services de sécurité et couches OSI

Le présent paragraphe décrit la façon dont les couches OSI sont utilisées pour assurer les services de sécurité et, par conséquent, montre comment ils peuvent être assurés efficacement dans les réseaux de télécommunication.

On suppose que si une couche assure un service de sécurité, ce service est assuré à la couche se trouvant au-dessus de la couche considérée. La fourniture de services par des couches exposée dans la Rec. UIT-T X.800 est utilisée comme base pour limiter les possibilités.

6.3.1 Authentification (entité homologue et origine des données)

Les couches suivantes peuvent assurer ce service (selon la Rec. UIT-T X.800):

– couche Réseau (confirmation de l'identité des homologues de couche Transport);
– couche Transport (confirmation de l'identité des homologues de couche Session);
– couche Application (confirmation de l'identité des processus d'application);
– hors de l'OSI (dans le processus d'application lui-même).

6.3.2 Contrôle d'accès

– *Contrôle d'accès de l'association de gestion*

  Ce service est utilisable aux niveaux où une association existe; cela aura lieu à la couche Application (contrôle d'accès pour les processus d'application) ou dans le processus d'application lui-même.

  Le contrôle d'accès d'association peut être assuré au niveau de la couche Réseau. En outre, le contrôle d'accès d'association peut être assuré au niveau de la couche Application ou dans le processus d'application lui-même.

– *Contrôle d'accès de notification de gestion*

  Ce service peut être utilisé au niveau de la couche Application ou dans le processus d'application lui-même, étant donné que le processus d'application lui-même peut faire la distinction entre des entités (du processus d'application) tels les gestionnaires et les agents.

– *Contrôle d'accès aux ressources gérées*

  Ce service peut être utilisé au niveau de la couche Application ou dans le processus d'application lui-même, étant donné que le processus d'application peut faire la distinction entre des entités (du processus d'application) tels les gestionnaires et les agents.

6.3.3 Alarme de sécurité, suivi d'audit et rétablissement

Ces services sont liés à d'autres services et par conséquent présents dans les couches où les autres services existent.

6.3.4 Intégrité

– *Intégrité sélective des champs*

  Ce service peut être utilisé dans la couche Application ou dans le processus d'application lui-même, étant donné que c'est le processus d'application qui peut faire la distinction entre les champs.

– *Intégrité des connexions avec rétablissement*

  Peut être assurée dans la couche Transport, au niveau de la couche Application ou dans le processus d'application.

– *Intégrité des connexions sans rétablissement*

  Peut être assurée au niveau de la couche Réseau, de la couche Transport, de la couche Application ou dans le processus d'application lui-même.

6.3.5 Confidentialité

– *Confidentialité sélective des champs*

  Ce service peut être utilisé dans la couche Application ou dans le processus d'application lui-même, étant donné que le processus d'application peut faire la distinction entre les champs.

– *Confidentialité des connexions et sans connexion*

  Considérant qu'il est nécessaire d'avoir une confidentialité de bout en bout, ce qui exclut la couche Physique et la couche Liaison de données, la confidentialité peut être assurée au niveau de la couche Réseau, de la couche Transport, de la couche Présentation, de la couche Application ou dans le processus d'application.

– *Confidentialité du flux de trafic*

  Ce service peut être assuré dans les couches Réseau, Transport ou Application ou dans le processus d'application lui-même.

6.3.6 Non-répudiation

– Non-répudiation – preuve de l'envoi;

– Non-répudiation – preuve de la remise.

  Ce service peut être utilisé dans la couche Présentation, la couche Application ou dans le processus d'application lui-même.

Ceci est résumé dans le Tableau 5. Ce Tableau est différent du Tableau 2 de la Rec. UIT-T X.800 en raison des domaines d'application différents des deux Recommandations.

Tableau 5/E.408 – Relation entre les services de sécurité et le modèle de référence OSI

	Couche						
Service	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Authentification de l'utilisateur	–	–	–	–	–	–	+
Authentification de l'entité homologue	–	–	+	+	–	–	+
Authentification de l'origine des données	–	–	+	+	–	–	+
Contrôle d'accès d'association de gestion	–	–	+	–	–	–	+
Contrôle d'accès de notification de gestion	–	–	–	–	–	–	+
Contrôle d'accès des ressources gérées	–	–	–	–	–	–	+
Alarme de sécurité, suivi d'audit et rétablissement	+	+	+	+	+	+	+
Intégrité sélective des champs	–	–	–	–	–	–	+
Intégrité des connexions avec rétablissement	–	–	–	+	–	–	+
Intégrité des connexions sans rétablissement	–	–	+	+	–	–	+
Confidentialité sélective des champs	–	–	–	–	–	–	+
Confidentialité avec connexion/sans connexion	–	–	+	+	–	+	+
Confidentialité des flux de trafic	–	–	+	+	–	+	+
Non-répudiation – preuve de l'envoi	–	–	–	–	–	+	+
Non-répudiation – preuve de la remise	–	–	–	–	–	+	+

6.4 Gestion de la sécurité

La gestion de la sécurité englobe toutes les activités visant à établir, maintenir et mettre fin aux aspects sécurité d'un système.

Les sujets concernés sont les suivants:

– gestion des services de sécurité;
– mise en place des mécanismes de sécurité;
– gestion des clés (partie gestion);
– création des identités, des clés, des informations de contrôle d'accès, etc.;
– gestion du suivi d'audit de sécurité et des alarmes de sécurité;
– prise de conscience et formation concernant la sécurité;
– stratégie de sécurité;
– politiques et règlements relatifs à la sécurité;
– gestion coopérative de la sécurité.

Appendice I

Aspects juridiques

I.1 Introduction

Le présent paragraphe décrit les domaines de la législation susceptibles d'influencer la normalisation de la sécurité dans les réseaux de télécommunication et tente d'en donner certaines conséquences.

I.2 Domaine de la législation applicable

Les domaines suivants de la législation susceptibles d'influencer la normalisation de la sécurité des réseaux de télécommunication ont été identifiés, à savoir:

Confidentialité

– "confidentialité de la correspondance": interdire l'accès par des tiers non autorisés aux informations échangées entre clients;

– limitation en matière de collecte, de stockage et de traitement de données personnelles: les données personnelles ne peuvent être collectées, stockées et traitées que s'il existe une relation entre les données et la fourniture réelle des services;

– divulgation: obligation faite à un opérateur de réseau d'interdire l'accès par des tiers non autorisés aux informations concernant les clients;

– "inspection et correction": le droit d'un client d'inspecter et de corriger les informations sur lui-même stockées, si c'est justifié, par un opérateur de réseau.

La législation concernant la confidentialité influencera principalement les conditions de sécurité concernant le contrôle d'accès, l'intégrité et la confidentialité.

Caractère contractuel

– la possibilité d'utiliser les informations concernant les échanges par réseau de télécommunication entre entités dans le cas d'un différend devant un tribunal;

– la reconnaissance par les tribunaux d'un contrat remis électroniquement.

Ce sont principalement les prescriptions de sécurité concernant l'intégrité et la non-répudiation qui seront concernées.

Sécurité internationale et ordre public national

– les demandes concernant une protection de l'information et de l'infrastructure: garantir la disponibilité et l'intégrité du réseau de télécommunication;

– les restrictions relatives à l'utilisation des méthodes cryptographiques: certains pays ont des législations qui limitent l'utilisation du chiffrement;

– l'obligation faite aux opérateurs de réseau de coopérer et de fournir des informations en cas d'interception licite, pour les enquêtes criminelles.

Cette législation peut influencer les prescriptions de sécurité. L'influence de la législation relative aux écoutes légales sur ces prescriptions est quelque peu confuse. Il y a toutefois une relation avec la confidentialité: par exemple, seules les informations relatives à une personne faisant l'objet d'une enquête doivent être fournies.

I.3 Origines de la législation

Dans le paragraphe précédent, la législation a été classée en sujets. Seront identifiées ci-après quelques sources de la législation et leur éventuelle influence sur la sécurité des réseaux de télécommunication.

– *Les Constitutions*

  Couvrant le secret de la correspondance, le secret de la vie privée, le droit à la liberté personnelle. Toutes les Constitutions ne font pas spécifiquement référence aux télécommunications.

– *Les traités internationaux*

  Deux exemples sont constitués par les traités de Rome et de Maastricht. Deux domaines de la législation sont importants ici pour les télécommunications. Le premier domaine concernant le marché européen (appelé "premier pilier") qui vise à établir une concurrence sur le marché (des télécommunications): sont importantes pour la sécurité "les prescriptions essentielles" sur la sécurité et l'intégrité des réseaux et sur la protection des données. Le deuxième domaine ("troisième pilier") porte sur la coopération européenne en matière de justice. Les points principaux concernant la sécurité sont les prescriptions relatives aux écoutes légales. Ces prescriptions portent sur le contenu des communications, les données associées aux communications et la localisation des cibles. On peut citer, en ce qui concerne la sécurité des réseaux de télécommunication: *la nécessité de dispositions spécifiques concernant la confidentialité, l'intégrité et l'écoute dans le processus d'écoute*.

– *Autres conventions internationales*

  Un grand nombre de ces conventions traite des droits humains, pour les télécommunications – parmi lesquels les plus importants sont la confidentialité et le secret. Les lois relatives à la propriété intellectuelle ne sont pas considérées comme relevant de la sécurité des réseaux de télécommunication.

– *Législation nationale*

  Les lois applicables traitent ici encore de la confidentialité, du secret et de l'écoute légale.

– *Règles établies par l'Organe national de réglementation des télécommunications*

  L'Organe national de réglementation des télécommunications est l'organe national (désigné par la législation nationale) auquel est conférée l'autorité d'émettre des règles et des règlements dans le domaine des télécommunications. Ces règles peuvent inclure des aspects relatifs à la sécurité.

– *Codes de pratiques*

  Il s'agit des politiques agréées entre les entreprises et organismes de télécommunication pour traiter des questions relatives à la sécurité. Pour la sécurité des réseaux de télécommunication, ces codes de pratiques peuvent revêtir une grande importance lorsque les réseaux de télécommunication sont interconnectés.

I.4 Conséquences possibles sur la normalisation de la sécurité des réseaux de télécommunication

Pour la normalisation de la sécurité des réseaux de télécommunication, les conséquences suivantes de la législation sont envisagées et doivent être prises en considération:

– la législation peut se traduire par des prescriptions concernant l'efficacité et la disponibilité des services de sécurité. Les paragraphes précédents donnent certaines indications concernant ces prescriptions;

– nécessité de fournir un certain niveau d'intégrité du réseau de télécommunication;

– possibilité de prendre en charge l'écoute légale et l'accès aux données de gestion pour les services de justice. La durée pendant laquelle les données peuvent devoir être stockées, et les processus permettant de garantir que les données sont détruites si nécessaires;
– dans certains pays, la législation peut interdire l'utilisation du cryptage;
– la législation ne sera pas la même dans tous les pays. Cela signifie que dans certains pays des prescriptions différentes peuvent apparaître.

Appendice II

Classes fonctionnelles et profils de sécurité

II.1 Regroupement des mesures de sécurité

Les mesures de sécurité peuvent être regroupées en "Classes fonctionnelles" (FC, *functional class*). La définition ci-après n'inclut pas l'efficacité d'une mesure de sécurité:

Une classe fonctionnelle est un ensemble homogène de mesures de sécurité visant à répondre aux prescriptions de sécurité de divers niveaux (fonctionnels).

II.1.1 Cas interdomaines: utilisation des classes fonctionnelles

La sécurité d'un réseau de télécommunication ne devrait pas être affectée par des activités interdomaines. Les règles applicables à l'interaction entre domaines devraient être définies dans une politique de sécurité interdomaines. Ces règles définiront des mesures de sécurité à appliquer pour un cas donné. Pour faciliter la compatibilité entre les divers domaines d'interaction, ces mesures de sécurité peuvent se référer à une classe fonctionnelle particulière.

II.1.2 Cas intradomaine: utilisation des classes fonctionnelles

Dans le cas intradomaine, les classes fonctionnelles peuvent faciliter la définition de la sécurité. Ces classes peuvent également être utilisées pour l'assurance de la sécurité. Pour cela, les classes fonctionnelles doivent être associées avec un niveau d'assurance déclaré par le fabricant de produits de gestion. Ce sujet a des relations fortes avec les critères d'évaluation formels.

Il se peut que, pour l'interaction interdomaines, un opérateur exige l'application d'une classe fonctionnelle particulière pour le cas intradomaine de l'autre opérateur. Cela peut s'expliquer par le fait que toutes les menaces peuvent être efficacement analysées à l'interface de deux domaines. Une solution consisterait à garantir la présence d'un niveau minimal de sécurité interne pour des réseaux de télécommunication en interaction. Une norme de sécurité des réseaux de télécommunication ne devrait pas prescrire que des classes fonctionnelles sont requises, mais devrait plutôt permettre la possibilité d'exiger la présence de certaines classes fonctionnelles, en définissant les éléments appropriés à sélectionner.

II.2 Classes fonctionnelles

Les classes fonctionnelles sont utilisées pour définir un groupe concis de services de sécurité destiné à répondre à un certain niveau de sécurité. Dans le présent paragraphe, on élabore un ensemble de classes fonctionnelles pour illustrer la façon dont ces classes peuvent être définies. On propose des classes fonctionnelles *pour l'interface-X* à trois niveaux de sécurité distincts:

1) la classe fonctionnelle minimale: (FC 1);
2) la classe fonctionnelle de base: (FC 2);
3) la classe fonctionnelle élaborée: (FC 3).

Pour des raisons pratiques, le nombre de classes fonctionnelles ne devrait pas être trop élevé. Par ailleurs, il devrait être possible de répondre aux prescriptions d'un nombre d'organisations différentes. Les classes fonctionnelles peuvent être modifiées comme suit:

– les classes fonctionnelles définies uniquement pour l'interface-X peuvent aussi porter sur les interfaces Q;

– la confidentialité est supposée être une caractéristique optionnelle pour toutes les classes et ceci pour deux raisons:
  - il s'agit d'une prescription moins stricte;
  - l'inclusion obligatoire dans une classe fonctionnelle peut avoir des conséquences légales concernant la possibilité d'utilisation de la classe.

Le Tableau II.1 contient un aperçu général des classes fonctionnelles.

Tableau II.1/E.408 – Classes fonctionnelles des services de sécurité

FC 1	FC 2	FC 3
Accent mis sur l'intégrité des ressources gérées stockées	Accent mis sur l'intégrité des ressources gérées, stockées et sur l'intégrité des données transférées	FC 2 plus justification des opérations de gestion
• Authentification (entité homologue et utilisateur) • Contrôle d'accès d'association de gestion • Contrôle d'accès aux ressources gérées • Alarme de sécurité, audit et rétablissement	• Authentification (entité homologue et utilisateur) • Contrôle d'accès d'association de gestion • Contrôle d'accès aux ressources gérées • Authentification de l'origine des données • Intégrité sélective des champs • Intégrité des connexions • Alarme de sécurité, audit et rétablissement	• Authentification (entité homologue et utilisateur) • Contrôle d'accès d'association de gestion • Contrôle d'accès aux ressources gérées • Authentification de l'origine des données • Intégrité sélective des champs • Intégrité des connexions • Non-répudiation de la source • Non-répudiation de la destination • Alarme de sécurité, audit et rétablissement
En option: • intégrité des connexions • confidentialité des connexions	En option: • confidentialité des connexions • confidentialité sélective des champs	En option: • confidentialité des connexions • confidentialité sélective des champs

En outre, une distinction doit être faite entre les classes fonctionnelles correspondant au cas interdomaines et les classes fonctionnelles correspondant au cas intradomaine. Les prescriptions peuvent être différentes dans les deux cas et c'est la raison pour laquelle aussi les mesures de sécurité peuvent être différentes.

La partie suivante donne un aperçu général des différents cas de sorte qu'il est possible de déterminer les classes fonctionnelles qui sont nécessaires et lesquelles sont applicables.

Hypothèse

Pour chaque domaine, il existe une autorité qui a la responsabilité de décider des mesures de sécurité à appliquer dans le domaine.

On distingue trois cas:

1) les classes fonctionnelles définies par une autorité responsable du domaine et applicables à ce propre domaine (intradomaine);
2) les classes fonctionnelles définies par une autorité responsable du domaine et applicables aux interactions entre domaines (interdomaines). Ces classes fonctionnelles résulteront d'un accord entre les autorités responsables des domaines en interaction;
3) les classes fonctionnelles définies par une autorité responsable du domaine sous forme de prescriptions applicables à la sécurité de l'autre domaine.

Dans chaque cas, il est possible d'identifier le nombre de classes correspondant à différents niveaux de sécurité.

Le nombre de niveaux de sécurité appelle un complément d'étude.

L'ensemble des mesures de sécurité qui forment une classe fonctionnelle appelle un complément d'étude.

Les classes fonctionnelles dans les différents cas peuvent être les mêmes, ce qui diminue le nombre total de classes.

On peut également envisager un compromis entre les différents cas, par exemple lorsque le niveau de la sécurité interdomaines est élevé, les prescriptions pour la sécurité interne dans l'autre domaine peuvent être moins grandes et inversement. Une autre possibilité serait qu'une classe fonctionnelle représente un ensemble minimal de mesures de sécurité qui peuvent être étendues le cas échéant par des mesures additionnelles.

II.3 Profils de sécurité

Les classes fonctionnelles n'imposent pas l'utilisation de mécanismes de sécurité normalisés; on peut appliquer tout mécanisme qui répond aux prescriptions.

Pour permettre l'interaction entre des mesures de sécurité de différents domaines, les mesures doivent être conformes à des normes. Une prescription relative à l'utilisation de normes particulières qui ensemble définissent une classe fonctionnelle est appelée profil de sécurité.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
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