Union internationale des télécommunications

UIT-T M.3016.0

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

(05/2005)

SÉRIE M: GESTION DES TÉLÉCOMMUNICATIONS Y COMPRIS LE RGT ET MAINTENANCE DES RÉSEAUX

Réseau de gestion des télécommunications

Sécurité pour le plan de gestion: aperçu général

Recommandation UIT-T M.3016.0

RECOMMANDATIONS UIT-T DE LA SÉRIE M

GESTION DES TÉLÉCOMMUNICATIONS Y COMPRIS LE RGT ET MAINTENANCE DES RÉSEAUX

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 télécommunication mobile	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 de 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.3016.0

Sécurité pour le plan de gestion: aperçu général

Résumé

La présente Recommandation fournit un aperçu général et un cadre qui identifient les menaces de sécurité concernant un RGT et résume la manière dont les services de sécurité disponibles peuvent s'appliquer dans le cadre général de l'architecture du RGT.

Source

La Recommandation UIT-T M.3016.0 a été approuvée le 22 mai 2005 par la Commission d'études 4 (2005-2008) de l'UIT-T selon la procédure définie dans la Recommandation UIT-T A.8.

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 M.3016.0

Sécurité pour le plan de gestion: aperçu général

1 Domaine d'application

La présente Recommandation fournit un aperçu général et un cadre qui identifient les menaces de sécurité concernant un RGT et résume la manière dont les services de sécurité disponibles peuvent s'appliquer dans le cadre général de l'architecture du RGT, telle que cette dernière est décrite dans la Rec. UIT-T M.3010.

La présente Recommandation est de nature générique et n'identifie ou ne concerne pas des prescriptions pour une interface de RGT spécifique.

La présente Recommandation ne tente pas de définir de nouveaux services de sécurité, mais utilise des services de sécurité existants définis dans d'autres Recommandations UIT-T et Normes internationales ISO.

La présente Recommandation appartient aux Recommandations UIT-T de la série M.3016.x destinées à fournir des lignes directrices et des prescriptions permettant de sécuriser le plan de gestion de réseaux évolutifs:

Rec. UIT-T M.3016.0 – *Sécurité pour le plan de gestion: aperçu général*.

Rec. UIT-T M.3016.1 – *Sécurité pour le plan de gestion: prescriptions de sécurité*.

Rec. UIT-T M.3016.2 – *Sécurité pour le plan de gestion: services de sécurité*.

Rec. UIT-T M.3016.3 – *Sécurité pour le plan de gestion: mécanisme de sécurité*.

Rec. UIT-T M.3016.4 – *Sécurité pour le plan de gestion: formulaire de sécurité*.

Les Recommandations UIT-T M.3016.1, M.3016.2 et M.3016.3 spécifient un ensemble de prescriptions, de services et de mécanismes permettant d'assurer de manière appropriée la sécurité des fonctions de gestion nécessaires à la prise en charge de l'infrastructure de télécommunications. Les diverses administrations et organisations nécessitant différents niveaux de prise en charge de sécurité, les Recommandations UIT-T M.3016.1, M.3016.2 et M.3016.3 ne précisent pas si une prescription, un service ou un mécanisme est obligatoire ou facultatif.

Le formulaire de sécurité défini dans la Rec. UIT-T M.3016.4 est destiné à aider les organisations, les administrations et d'autres organisations nationales/internationales à spécifier le caractère obligatoire ou facultatif de la prise en charge des prescriptions et les gammes de valeurs, les valeurs, etc., en vue d'implémenter leurs politiques de sécurité.

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 E.408 (2004), *Prescriptions de sécurité des réseaux de télécommunication*.

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

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

– Recommandation UIT-T X.509 (2000), *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), *Technologies de l'information – Interconnexion des systèmes ouverts – Gestion-systèmes: objets et attributs de 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), *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 – Cadres de sécurité pour les 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: cadre de 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: cadre de confidentialité*.

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

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

3 Définitions

La présente Recommandation ne définit aucun nouveau terme.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations suivantes:

CCITT Comité consultatif international télégraphique et téléphonique

FC classes fonctionnelles (*functional classes*)

ISO Organisation Internationale de Normalisation (*International Organization for Standardization*)

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

MF fonction de médiation (*mediation function*)

NEF fonction d'élément de réseau (*network element function*)

OSF fonction de système d'exploitation (*operation system function*)

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

PIN numéro d'identification personnel (*personal identification number*)

RCD réseau de communication de données

RGT réseau de gestion des télécommunications

TF fonction de transformation (*transformation function*)

TTP tiers de confiance (*trusted third party*)

UIT-T Union internationale des télécommunications – Secteur de la normalisation des télécommunications

WSF fonction de poste de travail (*workstation function*)

5 Motivations

Les définitions de besoins de sécurité dans un RGT sont issues des diverses sources suivantes:

– Les **clients** et **abonnés** qui ont des besoins de confidentialité pour le réseau et les services offerts, y compris une taxation correcte.

– La **communauté** et les **autorités publiques** qui formulent des prescriptions réglementaires et légales de sécurité afin de garantir la disponibilité des services équitable et le respect de la vie privée.

– Les **opérateurs de réseau** et les **fournisseurs de services** ont également des besoins de sécurité pour leur propre compte pour protéger leur exploitation et leurs intérêts commerciaux, ainsi que pour faire face à leurs obligations vis-à-vis des abonnés et du public.

L'objectif d'un RGT est la gestion du réseau de télécommunication sous-jacent; il s'ensuit que la sécurité du RGT est indispensable pour un fonctionnement correct du réseau de télécommunication en question. Le réseau de télécommunication peut en outre incorporer des fonctionnalités de sécurité qui ont besoin d'être gérées par le RGT. Les fonctions de gestion de la sécurité sont énumérées dans la Rec. UIT-T M.3400.

Les normes de sécurité du RGT doivent se baser de préférence sur des normes de sécurité qui ont fait l'objet d'un accord international; il est en effet préférable de réutiliser ces normes plutôt que d'en créer de nouvelles. La fourniture de l'utilisation de services et de mécanismes de sécurité peut entraîner des coûts élevés par rapport à la valeur des transactions devant être protégées. Il est donc important de pouvoir personnaliser la sécurité fournie à des transactions RGT protégées. Les services et mécanismes de sécurité utilisés pour sécuriser des transactions RGT doivent être fournis de manière à permettre une telle personnalisation. Compte tenu du grand nombre de combinaisons possibles pour les fonctionnalités de sécurité, il est souhaitable de disposer de **profils de sécurité** qui couvrent un large domaine d'applications de sécurité du RGT (se référer à l'Appendice I).

La normalisation facilitera la **réutilisation de solutions et de produits**, ce qui permettra une introduction plus rapide et plus économique des fonctions de sécurité.

Les vendeurs et les utilisateurs de systèmes retireront des avantages importants de la normalisation des solutions de systèmes du fait des économies d'échelle réalisées lors de l'élaboration des produits et de la possibilité d'interfonctionnement des composants au sein du RGT.

Il est nécessaire de fournir des services et des mécanismes de sécurité permettant de protéger les transactions RGT entre entités RGT (définies dans la Rec. UIT-T M.3010) contre des attaques malveillantes telles que les écoutes indiscrètes, les parodies, les altérations de messages (modification, retard, suppression, insertion, répétition, réacheminement, acheminement incorrect

ou modification de l'ordre des messages), les répudiations ou les falsifications. La protection englobe la prévention, la détection et le rétablissement après les attaques, ainsi que la gestion d'informations liées à la sécurité. Les normes doivent traiter aussi bien les interfaces (Q et F) intradomaine que les interfaces (X) interdomaine.

6 Description du système

La présente Recommandation a pour objectif de fournir une représentation abstraite permettant de masquer les détails d'implémentation et d'établir un accord sur des résultats correspondant ultérieurement à des implémentations spécifiques.

Le RGT est décrit par son architecture fonctionnelle, son architecture informationnelle et son architecture physique (se référer à la Rec. UIT-T M.3010).

La Rec. UIT-T M.3010 tient compte du fait que les blocs de construction du RGT peuvent prendre en charge d'autres interfaces en plus des interfaces Q, X et F. Les informations physiques peuvent de même concerner des fonctionnalités supplémentaires par rapport à celles qui transitent sur des interfaces Q, X et F. Ces interfaces supplémentaires et les fonctionnalités connexes sont en dehors du domaine d'application du RGT et, par voie de conséquence, en dehors du domaine d'application de la normalisation de la sécurité du RGT.

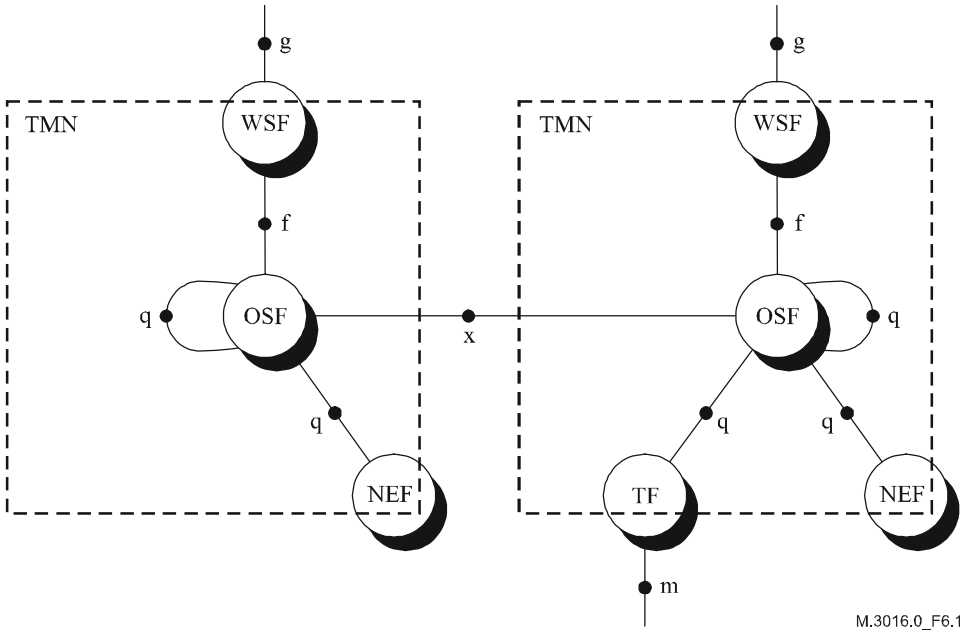

Figure 1/M.3016.0 – Architecture fonctionnelle du RGT

6.1 Acteurs et rôles

Seule la sécurité technique sera prise en considération aux fins de la normalisation de la sécurité du RGT, ce qui signifie que les acteurs pertinents sont les *utilisateurs du RGT*. Un utilisateur du RGT est une personne ou un processus qui met en œuvre des services de gestion du RGT en vue de mener à bien des opérations de gestion. Les utilisateurs du RGT peuvent être classés en utilisateurs internes appartenant à l'organisme qui exploite le RGT et en utilisateurs externes accédant au RGT.

L'utilisateur du RGT jouera un rôle chaque fois qu'il accède à un service de gestion. Il existera dans certains cas une relation un vers un entre un utilisateur du RGT et un rôle, c'est-à-dire que l'utilisateur du RGT jouera toujours le même rôle. Dans d'autres cas, la relation sera du type un vers plusieurs entre un utilisateur du RGT donné et les rôles qu'il peut remplir.

La liste suivante présente un classement général de certains rôles usuels:

– opérateurs de réseau (*privés ou publics*);
– fournisseurs de services (*services supports ou services à valeur ajoutée*);
– abonnés ou clients du service;
– utilisateurs du service finaux;
– fournisseurs d'équipements ou de logiciels;
– tiers de confiance (c'est-à-dire un tiers qui bénéficie de la confiance des deux parties et qui agit conformément aux lois et aux réglementations nationales pour assurer la certification, l'authentification et les services connexes).

Il est important, du point de vue de la sécurisation du RGT, de contrôler non seulement le comportement d'utilisateurs connus, mais également de prendre en considération la possibilité d'une tentative d'accès non autorisé au RGT par un intrus.

Certaines mesures de sécurité peuvent nécessiter des acteurs jouant le rôle de tiers de confiance (TTP, *trusted third party*). La manière dont ces acteurs sont autorisés à interagir avec le RGT constitue un problème de sécurité important.

6.2 Domaines de sécurité

La Rec. UIT-T M.3010 introduit le concept d'architecture logique en couches (LLA, *logical layered architecture*), dans laquelle les fonctionnalités de gestion sont réparties dans des couches. Chaque couche traite un sous-ensemble bien défini de la totalité des activités de gestion. Chaque couche fonctionnelle constituera un domaine de gestion distinct, appelé domaine OSF, qui se trouve sous la commande d'une fonction de système d'exploitation (OSF, *operation system function*). Des fonctions d'élément réseau (NEF, *network element function*) commandées par la fonction OSF feront partie du domaine OSF. Un RGT sera constitué d'un ou de plusieurs domaines OSF qui peuvent être disjoints ou avoir des relations d'interaction, de recouvrement ou de contenu.

Un *domaine de sécurité* est un ensemble d'entités et de participants qui sont soumis à une même politique de sécurité et à une même administration de la sécurité. Une hypothèse normale consiste à considérer un RGT comme un domaine de sécurité unique. Ceci sera souvent le cas, mais cette hypothèse ne doit pas être généralisée. Des RGT de taille importante peuvent avoir des besoins de sécurité divers et être soumis à diverses politiques de sécurité. Il semble donc être plus approprié de considérer qu'un domaine de sécurité du RGT contient un seul domaine OSF ou un ensemble de tels domaines.

Les relations de sécurité intradomaine et interdomaine suivantes s'appliquent compte tenu de cette hypothèse:

Relations de sécurité intradomaine possibles:

– q (OSF-NEF, OSF-OSF).

Relations de sécurité interdomaine possibles:

– x (OSF-OSF);
– f (WSF-OSF, WSF-MF);
– q (OSF-OSF, OSF-TF).

Il convient de noter que les relations précédentes concernent des domaines de sécurité et non des domaines de gestion. Il est important de noter également qu'un point de référence q peut être impliqué aussi bien dans des relations de sécurité interdomaine que dans des relations de sécurité intradomaine. Le degré de confiance entre les entités impliquées constitue une des différences principales entre ces deux types de relation.

7 Objectifs génériques de sécurité pour le RGT

Le présent paragraphe a pour but de décrire l'objectif final des mesures de sécurité qui sont prises dans un environnement se conformant à la normalisation du RGT. L'accent sera mis sur la sécurité obtenue plutôt que sur la manière dont cette dernière est atteinte.

Les objectifs de sécurité doivent être définis en partant des préoccupations de l'opérateur et des autres acteurs, de leurs relations commerciales, de contraintes légales et réglementaires, de contraintes contractuelles, etc.

Les objectifs de sécurité du RGT sont les suivants:

– Seuls des acteurs légitimes doivent disposer de la possibilité d'accès et de traitement concernant des biens qui se trouvent au sein d'un RGT.
– Les acteurs légitimes doivent disposer de la possibilité d'accès et de traitement concernant les biens pour lesquels ils possèdent une autorisation d'accès.
– Tous les acteurs doivent pouvoir être rendus responsables de leurs actions au sein du RGT et de ces seules actions.
– La disponibilité du RGT doit être protégée contre des accès ou des actions non sollicitées.
– Il doit être possible d'extraire du RGT des informations relatives à la sécurité.
– Lorsque des violations de sécurité sont détectées, il doit être possible de les traiter d'une manière contrôlée afin de minimiser les dégâts.
– Il doit être possible de restaurer les niveaux normaux de sécurité après une rupture de la sécurité.
– L'architecture de sécurité du RGT doit être suffisamment souple pour prendre en charge diverses politiques de sécurité, par exemple, des mécanismes de sécurité de force différente.

Le terme "accéder à des biens" signifie qu'il est possible non seulement d'exécuter des fonctions mais également de lire des informations.

Les besoins génériques sont exprimés du point de vue et avec les termes de la gestion de l'entreprise. Les paragraphes qui suivent doivent être exprimés dans des termes plus techniques qui conduisent à la définition de services et de fonctions de sécurité susceptibles d'être implémentés. Le mappage entre les deux terminologies n'est pas toujours évident.

Il est possible de démontrer que les cinq premiers objectifs de sécurité du RGT mentionnés ci-dessus dans le présent paragraphe seront satisfaits s'il est possible de satisfaire à l'ensemble des objectifs de sécurité suivants:

– confidentialité;
– intégrité des données;
– responsabilité;
– disponibilité.

Les menaces et risques identifiés dans le § 9 et les prescriptions fonctionnelles du § 6 seront basés sur ces termes plus formels. Se référer au § 9 en ce qui concerne les définitions.

8 Problèmes de législation

L'infrastructure de sécurité d'un RGT doit être en mesure de s'adapter aux contraintes imposées par les lois gouvernementales, la législation contractuelle, les traités et la réglementation. Ces contraintes peuvent porter sur des services de sécurité obligatoires (tels que la garantie de la confidentialité des informations des clients), l'interdiction de certains mécanismes de sécurité (tels que certains types de chiffrement) ou la prise en charge d'écoutes discrètes par des organismes d'application de la loi.

9 Menaces et risques

Le présent paragraphe a pour but d'examiner les menaces et les risques auxquels un RGT est exposé. Il n'a pas l'intention de spécifier une évaluation de risques ou une analyse de menaces pour une instance particulière de RGT. Il s'agit dans ce dernier cas d'un problème local qui peut être traité de manière différente par chaque fournisseur sans affecter l'interfonctionnement.

Une menace est une violation potentielle de la sécurité. Les menaces peuvent être dirigées contre quatre types d'objectifs différents, conformément aux objectifs spécifiques de sécurité identifiés pour le RGT:

– **confidentialité** (confidentialité des informations stockées et transférées);
– **intégrité des données** (protection des informations stockées et transférées);
– **responsabilité** (toute entité doit être responsable de toutes les actions qu'elle initialise);
– **disponibilité** (toute entité légitime doit obtenir un accès correct aux fonctionnalités du RGT).

La présente Recommandation distingue trois types de menaces:

– menaces accidentelles dont l'origine n'implique pas une intention malveillante;
– menaces administratives qui surviennent en raison d'une lacune dans l'administration de la sécurité;
– menaces intentionnelles qui impliquent une entité malveillante pouvant viser, soit la communication proprement dite, soit des ressources réseau.

Les menaces accidentelles et administratives peuvent être prises en compte par la normalisation du RGT dans la mesure où leurs conséquences sont les mêmes que celles des menaces intentionnelles. Une analyse plus précise des menaces prenant en compte l'architecture du RGT est faite dans la présente Recommandation en se concentrant sur les menaces intentionnelles qui visent la communication entre des acteurs du RGT. Cette démarche a pour but d'établir une liste plus concise de menaces qui peut être utilisée directement pour la normalisation du RGT. Une analyse des menaces concernant le RGT doit donc traiter les points suivants résultant de la Rec. UIT-T X.800:

– **imposture; usurpation d'identité**: une entité prétend être une entité différente;
– **écoutes (indiscrètes)**: violation de la confidentialité par surveillance de la communication;
– **accès non autorisé**: une entité tente 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 action non autorisée de suppression, d'insertion, de modification, de changement d'ordre, de répétition ou de création de retard;
– **répudiation**: une entité nie son implication dans un échange de communication antérieur;
– **falsification**: une entité crée de toutes pièces des informations dont elle prétend qu'elles ont été reçues d'une autre entité ou émises à destination d'une autre entité;
– **déni de service**: cette menace se présente lorsqu'une entité échoue dans l'exécution d'une fonction ou empêche d'autres entités d'exécuter leurs fonctions. Ceci peut concerner le déni de l'accès au RGT ou le déni de communication résultant d'une submersion du RGT. Dans un réseau partagé, cette menace peut être caractérisée par la création de trafic supplémentaire qui submerge le réseau, ce qui conduit à des retards dans le trafic empêchant les utilisateurs d'accéder au réseau.

Le Tableau 1 indique la correspondance entre les menaces et les objectifs.

Tableau 1/M.3016.0 – Mappage entre menaces et objectifs

Menace	Confidentialité	Intégrité des données	Responsabilité	Disponibilité
Imposture	x	x	x	x
Ecoutes indiscrètes	x			
Accès non autorisé	x	x	x	x
Perte ou altération d'informations (transférées)		x		x
Répudiation			x	
Falsification		x	x	
Déni de service				x

Une menace potentielle n'est pas dommageable pour un système tant que celui-ci ne possède pas une faiblesse correspondante au moment où une tentative est faite pour exploiter cette faiblesse. Toute menace implique un risque. L'évaluation d'un risque peut être subdivisée en une évaluation de la probabilité de chaque menace et une évaluation des conséquences possibles de la menace. L'évaluation des risques et des menaces doit être faite selon un processus itératif: de nouvelles menaces peuvent survenir lorsque des contre-mesures sont mises en œuvre, par exemple une menace sur des clés de chiffrement peut survenir lorsque des mesures de chiffrement sont prises.

10 Prescriptions et services de sécurité

La Figure 2 présente les relations entre les objectifs de sécurité, les menaces, les prescriptions de sécurité et les services. Elle décrit le processus permettant de déduire, à partir des menaces et des objectifs de sécurité, des prescriptions de sécurité qui se concrétiseront à leur tour par un ensemble de services de sécurité. Ces services de sécurité s'opposeront aux menaces et mettront en œuvre des mécanismes de sécurité qui utiliseront à leur tour des algorithmes de sécurité.

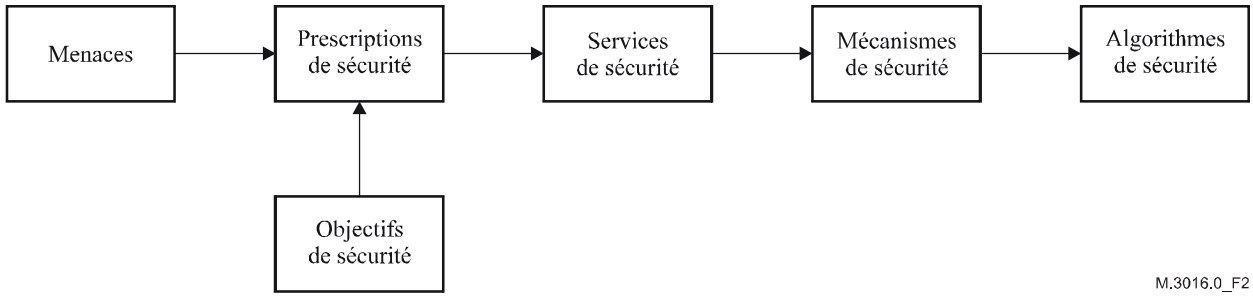

Figure 2/M.3016.0 – Cadre de sécurité

Le paragraphe 10.1 donne une liste de telles prescriptions de sécurité. Sauf indication contraire, le terme "prescription" dans la présente Recommandation ne signifie pas qu'une certaine fonctionnalité est toujours obligatoire pour tout RGT, mais plutôt qu'une fonctionnalité peut être rendue obligatoire par l'administration d'un RGT pour certaines applications spécifiques du RGT ou pour certaines interfaces du RGT, ou pour les deux. Le choix effectif dépendra des objectifs de sécurité exprimés dans la politique de sécurité de l'opérateur.

Il exprime en outre certaines prescriptions génériques pour la gestion des services de sécurité (voir le § 10.2) et des prescriptions architecturales qui régissent l'intégration de services de sécurité au sein du RGT (voir le § 10.3). Les prescriptions d'administration et de cycle de vie sont importantes mais ne seront pas traitées car elles n'affectent pas l'architecture.

10.1 Prescriptions de sécurité et services correspondants

Le présent paragraphe décrit un ensemble de prescriptions fonctionnelles génériques et les services correspondants pouvant être utilisés pour s'opposer à des menaces concernant un RGT.

10.1.1 Mappages entre prescriptions fonctionnelles, menaces et objectifs de sécurité

Le présent paragraphe identifie dans le Tableau 2 des prescriptions fonctionnelles de sécurité permettant de faire face aux menaces dont la liste est donnée par le § 9. Les prescriptions de sécurité ont ensuite été mappées (Tableau 3) avec les objectifs de sécurité mentionnés dans le § 7. Cette liste se limite à des prescriptions de nature générique qui ont un impact substantiel sur les composants et l'architecture.

Tableau 2/M.3016.0 – Mappage des prescriptions fonctionnelles et des menaces

Prescription fonctionnelle	Imposture	Ecoutes indiscrètes	Accès non autorisé	Perte ou altération d'informations	Répudiation	Falsification	Déni de service
Vérification d'identité	x		x				
Contrôle d'accès et d'autorisation			x				x
Protection de la confidentialité		x	x				
Protection de l'intégrité des données				x			
Responsabilité					x	x	
Journal d'activités	x		x		x	x	x
Compte rendu d'alarme	x		x	x			x
Audit	x		x		x	x	x

Le Tableau 3 donne l'ensemble des prescriptions fonctionnelles nécessaires pour atteindre les objectifs fonctionnels définis dans le § 3 et indiqués dans les colonnes.

10.1.2 Description des prescriptions fonctionnelles et des services correspondants

Les prescriptions fonctionnelles figurant dans les Tableaux 2 et 3 sont analysées plus en détail dans le texte qui suit et les services de sécurité correspondant à chacune des prescriptions sont identifiés. Il convient de noter que les prescriptions de l'une quelconque de ces fonctions n'invoquent pas de manière automatique un service de sécurité tel qu'il est défini par l'ISO. Il existe toutefois dans la pratique une concordance dans un certain nombre de cas.

Tableau 3/M.3016.0 – Mappage des objectifs de sécurité et des prescriptions fonctionnelles

Prescription fonctionnelle	Confidentialité	Intégrité des données	Responsabilité	Disponibilité
Vérification d'identité	x	x	x	
Contrôle d'accès et d'autorisation	x	x	x	x
Protection de la confidentialité	x			
Protection de l'intégrité des données		x		
Responsabilité			x	
Journal d'activités			x	x
Compte rendu d'alarme	x	x	x	x
Audit			x	x

10.1.2.1 Vérification d'identité

Un RGT doit fournir des capacités permettant d'établir et de vérifier l'identité déclarée par tout acteur du RGT.

Les acteurs sont des utilisateurs humains ou des entités au sein du RGT. Les identités vérifiées fournissent la base de la responsabilité et jouent un rôle essentiel dans la prise en charge de la plupart des prescriptions de sécurité analysées dans le présent paragraphe.

Le service de sécurité qui prend en charge la vérification des identités est l'**authentification**. Ce service fournit la preuve qu'un objet ou un sujet possède effectivement l'identité qu'il déclare. Les types d'authentification suivants peuvent être nécessaires en fonction du type d'acteur et du but de l'identification:

– authentification de l'utilisateur, fournissant la preuve de l'identité d'un utilisateur humain ou d'un processus d'application;
– authentification de l'entité homologue, fournissant la preuve de l'identité d'une entité homologue durant une relation de communication;
– authentification de l'origine des données, fournissant la preuve de l'identité du responsable d'une unité de données spécifique.

L'utilisation d'un service d'authentification fournit une preuve à un instant donné. La garantie de la continuité de la preuve nécessite la répétition de l'authentification dans le temps ou la constitution d'un lien avec un service d'intégrité.

Des exemples de mécanismes utilisés pour implémenter le service d'authentification sont l'authentification simple par mot de passe et numéro d'identification personnel (PIN, *personal identification number*) et l'authentification forte basée sur des méthodes de chiffrement.

10.1.2.2 Contrôle d'accès et d'autorisation

Un RGT doit fournir des capacités garantissant que les acteurs ne peuvent pas obtenir un accès à des informations ou des ressources pour lesquelles ils ne possèdent pas d'autorisation d'accès.

Le service de sécurité qui prend en charge cette prescription est le **contrôle d'accès**. Ce service fournit le moyen de garantir que l'accès à des ressources par les acteurs se fait uniquement de manière autorisée. Les ressources en question peuvent être le système physique, le logiciel système, les applications et les données. Le service de contrôle d'accès peut être défini et implémenté dans le RGT au niveau agent, au niveau objet ou au niveau attribut. Les limitations d'accès sont indiquées dans les informations de contrôle d'accès qui spécifient:

– les moyens permettant de déterminer quelles sont les entités qui disposent d'une autorisation d'accès;
– le type d'accès autorisé (lecture, écriture, modification, création, suppression).

Des contrôles d'accès plus spécifiques du RGT peuvent être subdivisés en trois types:

– *Contrôle d'accès à une association de gestion*

  Ce service permet le contrôle d'accès au niveau d'une association de gestion, ce qui signifie que les droits d'accès sont relatifs à l'association en elle-même, c'est-à-dire à l'autorisation d'établissement de l'association.

– *Contrôle d'accès à une notification de gestion*

  Ce service permet un contrôle d'accès portant sur les notifications, en assurant que les notifications ne sont visibles que pour des entités autorisées à les recevoir.

– *Contrôle d'accès à une ressource gérée*

  Ce service permet un contrôle d'accès concernant les ressources proprement dites.

L'identité de l'entité qui tente d'obtenir l'accès doit être vérifiée avant que l'accès à la ressource soit accordé. Ceci signifie que le contrôle d'accès est toujours lié à l'utilisation d'un service d'authentification.

10.1.2.3 Protection de la confidentialité

Un RGT doit fournir des capacités permettant d'assurer la confidentialité des données stockées et transmises.

Les services de sécurité prenant en charge cette prescription sont le **contrôle d'accès** aux données stockées et la **confidentialité des données** transmises. La **confidentialité des données** peut également être requise pour certains types de données stockées (les mots de passe, par exemple).

Le service de confidentialité fournit une protection contre la divulgation non autorisée de données échangées. On peut distinguer les types de service de confidentialité suivants:

– confidentialité sélective de champ;
– confidentialité de connexion;
– confidentialité de flux de données.

10.1.2.4 Protection de l'intégrité des données

Un RGT doit être en mesure de garantir l'intégrité des données stockées et transmises.

Les services de sécurité qui prennent en charge cette prescription sont le **contrôle d'accès** aux données stockées, l'**intégrité des données** stockées et la **confidentialité des données** transmises.

Le service d'intégrité fournit des moyens permettant d'assurer que les données échangées sont correctes en fournissant une protection contre la modification, la suppression, la création (insertion) et la répétition des données échangées. On peut distinguer les types de service d'intégrité suivants:

– intégrité sélective de champ;
– intégrité de connexion sans reprise;
– intégrité de connexion avec reprise.

10.1.2.5 Responsabilité

Un RGT doit fournir la capacité d'éviter qu'une entité puisse nier la responsabilité de toute action qu'elle a effectuée ainsi que de toute conséquence de cette action.

Cette prescription est prise en charge par le service de **non-répudiation** qui établit un lien entre l'individu (ou l'entité) et l'opération effectuée. Les services de non-répudiation fournissent un moyen permettant d'établir la preuve qu'un échange de données a effectivement eu lieu. Ils peuvent se présenter sous l'une des formes suivantes:

– non-répudiation: preuve de l'origine;

– non-répudiation: preuve de la livraison.

Une autre réalisation plus générale et éventuellement plus faible de la responsabilité est fournie par des combinaisons appropriées des services d'**authentification**, de **contrôle d'accès** et de **trace d'audit**.

10.1.2.6 Journal d'activités, compte rendu d'alarme et audit

Ces prescriptions répondent aux besoins de stockage et d'analyse concernant des activités au sein du RGT qui sont en relation avec la sécurité. Des notifications d'alarme doivent en outre être générées pour certains événements pouvant être sélectionnés. Les services adéquats sont la **trace d'audit** et le **compte rendu d'alarme**. Chacune de ces prescriptions est analysée ci-dessous de manière plus détaillée.

10.1.2.6.1 Journal d'activités

Un RGT doit fournir la capacité de stockage d'informations concernant des activités au sein du système, avec la possibilité de retrouver la trace entre ces informations et les entités ou individus impliqués.

Un journal constitue un recueil pour des enregistrements: il s'agit de l'abstraction OSI qui représente le journal d'utilisation des ressources pour des systèmes ouverts réels. Les enregistrements contiennent les informations journalisées.

Beaucoup de fonctions de gestion doivent être en mesure de conserver des informations au sujet d'événements qui se sont manifestés ou d'opérations qui ont été exécutées ou qui ont fait l'objet d'une tentative d'exécution pour des ressources diverses.

Il doit en outre être possible d'extraire ces informations du journal. Un gestionnaire devrait pouvoir être en mesure de déterminer si un enregistrement quelconque a été perdu ou si les caractéristiques des enregistrements stockés ont été modifiées à un moment quelconque.

10.1.2.6.2 Compte rendu d'alarme de sécurité

Un RGT doit fournir la capacité de générer des notifications d'alarme concernant des événements sélectionnés. L'utilisateur doit pouvoir définir les critères de sélection.

La fonction d'audit de sécurité est une fonction de gestion-systèmes qui décrit les notifications concernant un ensemble d'événements de sécurité. La notification d'alarme de sécurité définie par cette fonction de gestion-systèmes fournit des informations concernant l'état de fonctionnement du point de vue de la sécurité.

10.1.2.6.3 Audit de sécurité

Un RGT doit fournir la capacité d'analyser des données du journal de sécurité à des fins de contrôle portant sur les violations de la politique de sécurité.

Un audit doit être considéré comme une action indépendante de révision et d'examen d'enregistrements et d'activités du système qui a pour but de vérifier si les contrôles du système sont adéquats, d'assurer la conformité avec la politique de sécurité et les procédures de fonctionnement en vigueur et de détecter les infractions à la sécurité. Le résultat de l'audit peut identifier des modifications à apporter aux contrôles, aux politiques et aux procédures.

Le Tableau 4 donne un aperçu général concernant les relations entre les prescriptions et les services de sécurité. Le présent paragraphe définit uniquement les services de sécurité qui font l'objet de

solutions normalisées; d'autres services possibles ne sont pas examinés (par exemple, la détection du déni de service).

Tableau 4/M.3016.0 – Mappage entre prescriptions et services de sécurité

Prescription fonctionnelle	Service de sécurité
Vérification d'identité	authentification de l'utilisateur authentification d'entité homologue authentification de l'origine des données
Contrôle d'accès et d'autorisation	contrôle d'accès
Protection de la confidentialité – données stockées	contrôle d'accès confidentialité
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
Journal d'activités	trace d'audit
Compte rendu d'alarme de sécurité	alarme de sécurité
Audit de sécurité	trace d'audit
Protection du réseau RCD	inspection de paquets

NOTE – Les prescriptions qui suivent diffèrent de celles qui ont été énoncées dans le Tableau 4 et ne semblent pas être de manière évidente candidates pour une normalisation éventuelle. Elles doivent néanmoins être prises en considération lors de la phase de conception parallèlement à l'implémentation des prescriptions noyau du RGT énoncées précédemment.

10.1.2.6.4 Intégrité du système

Il est indispensable que les environnements logiciel et matériel des fonctions de sécurité implémentées maintiennent le niveau de sécurité requis.

Ceci englobe la configuration correcte des systèmes d'exploitation et l'élimination des défauts du système.

Ces points ne font pas partie du profil fonctionnel de sécurité proprement dit, mais ils doivent être énoncés simultanément aux spécifications de ce profil afin de garantir la résistance des fonctions dans un environnement réel.

10.1.2.6.5 Remarques concernant la disponibilité

La mise en œuvre d'une prescription concernant la disponibilité ne correspond pas à un service de sécurité unique ou à un ensemble restreint de tels services. Tous les services de sécurité énumérés doivent constituer un ensemble cohérent qui est globalement en mesure d'assurer la disponibilité. Des services de sécurité isolés ne seront pas en mesure de garantir la disponibilité car cette dernière est également influencée par la fiabilité du matériel et du logiciel (considérés du point de vue de la conception et de l'implémentation).

10.1.2.7 Protection du réseau RCD

Un RGT devrait assurer la protection du réseau RCD vis-à-vis du trafic client et du trafic de réseau homologue.

Un RGT devrait assurer l'isolement du trafic RCD vis-à-vis d'autres types de trafic, en particulier dans un réseau RCD à transmission en mode paquet.

10.2 Prescriptions concernant la gestion de la sécurité

Un RGT doit contenir des modèles d'information et des capacités de gestion pour les services utilisés en vue de sécuriser le RGT.

Des prescriptions détaillées de gestion de la sécurité indiquent quelles sont les applications de gestion à introduire et de quelle manière celles-ci doivent être conçues. Ceci permet de fournir au gestionnaire de sécurité les outils adéquats pour la supervision et la commande efficace et correcte des services de sécurité. Les objectifs de la gestion de la sécurité sont définis dans un système de télécommunication aux niveaux de la sécurité du système, des services de sécurité et des mécanismes de sécurité.

L'exploitation et les informations en rapport avec la gestion de services de sécurité dans un RGT nécessitent une attention particulière du point de vue de la sécurité. Les clés de chiffrement secrètes, les informations d'authentification et les listes de contrôle d'accès sont des exemples d'informations qui peuvent avoir besoin d'un niveau de protection plus élevé que la gestion du réseau.

La gestion de la sécurité doit être cohérente avec les fonctions de gestion de la sécurité définies dans la Rec. UIT-T M.3400.

Le rétablissement du système dans un état sécurisé doit être pris en charge après l'apparition d'une infraction à la sécurité.

Le RGT doit être en mesure, lorsqu'une infraction à la sécurité se présente, de traiter cette tentative d'une manière contrôlée, ce qui signifie que la tentative ne doit pas entraîner une dégradation grave de la disponibilité du RGT.

10.3 Prescriptions architecturales

Les besoins les plus importants à satisfaire pour l'adaptation des mesures de sécurité au cadre général du RGT sont les suivants:

– les mesures doivent être basées sur les principes du modèle fonctionnel du RGT;
– les mesures doivent être conformes au modèle de données par objet du RGT;
– les mesures doivent pouvoir s'appliquer à tout domaine du RGT dans les secteurs public et privé;
– les solutions doivent pouvoir être mises à l'échelle pour s'adapter à des RGT de taille importante ou réduite;
– les solutions doivent être compatibles avec l'architecture interne des points de référence du RGT pris en considération;
– les solutions doivent tenir compte des préoccupations de tous les utilisateurs internes ou externes du RGT;
– les solutions doivent prendre en considération les aspects de robustesse;
– les solutions doivent prendre en charge la reconfiguration par addition ou suppression d'utilisateurs ou d'applications.

Des conflits peuvent survenir entre le domaine de la sécurité et d'autres domaines fonctionnels. L'intégrité et la confidentialité des données de taxation doivent être mises en balance avec les besoins de débit créés par la quantité importante d'informations de tickets de taxation. Un ensemble de prescriptions de sécurité digne de confiance doit prendre en considération les effets éventuels des caractéristiques sur d'autres domaines fonctionnels.

D'autres besoins fonctionnels peuvent se manifester lors de l'analyse de scénarios spécifiques du RGT.

10.4 Services de sécurité et couches OSI

Le présent paragraphe indique quelles sont les couches OSI utilisées pour fournir les services de sécurité et, de ce fait, comment ces derniers peuvent être fournis pour un RGT de manière constructive.

On suppose qu'un service de sécurité présent dans une couche est fourni à la couche immédiatement supérieure. L'éventail des possibilités est réduit en utilisant comme base la fourniture de services par les couches décrites dans la Rec. UIT-T X.800.

10.4.1 Authentification de l'utilisateur

Ce service dépend d'une interaction avec l'utilisateur et se trouve de ce fait en dehors du domaine d'application du modèle OSI.

10.4.2 Authentification (entité homologue et origine des données)

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

– couche Réseau (corroboration de l'identité des entités homologues de la couche Transport);

– couche Transport (corroboration de l'identité des entités homologues de la couche Session);

– couche Application (corroboration de l'identité de processus d'application);

– hors OSI: dans le processus d'application lui-même.

Compte tenu du fait que la prescription pour le RGT sera d'identifier et d'authentifier les gestionnaires, les agents et le lien d'authentification avec le contrôle d'accès, les emplacements recommandés dans la pile OSI sont la couche Application et le processus d'application.

10.4.3 Contrôle d'accès

– *Contrôle d'accès à une association de gestion*

  Ce service est utilisable aux niveaux pour lesquels une association existe et qui seront la couche Application (contrôle d'accès pour les processus d'application) et le processus d'application lui-même.

  Le contrôle d'accès à l'application peut être fourni au niveau de la couche Réseau, par exemple en utilisant le service X.25 de groupement fermé d'utilisateurs. Le contrôle d'accès à l'association peut être fourni en outre au niveau de la couche Application ou par le processus d'application lui-même.

– *Contrôle d'accès à une notification de gestion*

  Ce service peut être utilisé au niveau de la couche Application ou par le processus d'application lui-même, étant donné que c'est ce dernier qui peut faire la distinction entre des entités (de processus d'application) telles que des gestionnaires et des agents.

– *Contrôle d'accès à une ressource gérée*

  Ce service peut être utilisé au niveau de la couche Application ou par le processus d'application lui-même, étant donné que c'est ce dernier qui peut faire la distinction entre des entités (de processus d'application) telles que des gestionnaires et des agents.

10.4.4 Alarme de sécurité, trace d'audit et rétablissement

Ces services sont fournis en liaison avec d'autres services et sont donc présents dans les mêmes couches que ces derniers.

10.4.5 Intégrité

– *Intégrité sélective de champ*

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

– *Intégrité de connexion avec rétablissement*

Ce service peut être fourni au niveau de la couche Transport, de la couche Application ou dans le processus d'application.

– *Intégrité de la connexion sans rétablissement*

Ce service peut être fourni au niveau de la couche Réseau, de la couche Transport, de la couche Application ou dans le processus d'application.

10.4.6 Confidentialité

– *Confidentialité sélective de champ*

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

– *Confidentialité avec ou sans connexion*

Une confidentialité de bout en bout est nécessaire, ce qui exclut la couche Physique et la couche Liaison de données; la confidentialité peut être fournie 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 fourni dans la couche Réseau, dans la couche Transport, dans la couche Application ou dans le processus d'application.

10.4.7 Non-répudiation

– Non-répudiation: preuve d'envoi.

– Non-répudiation: preuve de livraison.

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

Ces liaisons entre services et couches OSI sont résumées par le Tableau 5.

Tableau 5/M.3016.0 – Liaisons des services de sécurité avec le modèle de référence OSI

	Couche						
Service	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Authentification de l'utilisateur	–	–	–	–	–	–	+
Authentification d'entité homologue	–	–	+	+	–	–	+
Authentification de l'origine des données	–	–	+	+	–	–	+
Contrôle d'accès à une association de gestion	–	–	+	–	–	–	+
Contrôle d'accès à une notification de gestion	–	–	–	–	–	–	+
Contrôle d'accès à une ressource gérée	–	–	–	–	–	–	+
Alarme de sécurité, trace d'audit et rétablissement	+	+	+	+	+	+	+
Intégrité sélective de champ	–	–	–	–	–	–	+
Intégrité de connexion avec rétablissement	–	–	–	+	–	–	+
Intégrité de la connexion sans rétablissement	–	–	+	+	–	–	+
Confidentialité sélective de champ	–	–	–	–	–	–	+
Confidentialité avec ou sans connexion	–	–	+	+	–	+	+

Tableau 5/M.3016.0 – Liaisons des services de sécurité avec le modèle de référence OSI

	Couche						
Service	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Confidentialité de flux de trafic	–	–	+	+	–	+	+
Non-répudiation – preuve d'envoi	–	–	–	–	–	+	+
Non-répudiation – preuve de livraison	–	–	–	–	–	+	+

10.5 Gestion de la sécurité

La gestion de la sécurité englobe toutes les activités d'établissement, de maintien et de terminaison de caractéristiques de sécurité d'un système.

Les sujets suivants sont traités:

– gestion de services de sécurité;
– installation de mécanismes de sécurité;
– gestion des clés (partie de gestion);
– établissement d'informations d'identité, de clés, de contrôle d'accès, etc.;
– gestion de la trace de l'audit de sécurité et des alarmes de sécurité.

Appendice I

Classes fonctionnelles et sous-profils de sécurité

I.1 Regroupement de mesures de sécurité

Les mesures de sécurité peuvent être regroupées en "classes fonctionnelles" (FC, *functional classes*). La définition qui suit ne tient pas compte de la force d'une mesure de sécurité.

Une classe fonctionnelle est un ensemble cohérent de mesures de sécurité dont le but est de satisfaire des prescriptions de sécurité pour divers niveaux fonctionnels.

I.1.1 Utilisation de classes fonctionnelles entre domaines

La sécurité d'un RGT ne doit pas être affectée de manière négative par une activité interdomaine. Les règles d'interaction entre domaines doivent être définies dans une politique de sécurité interdomaine. Ces règles définiront quelles sont les mesures de sécurité qui doivent être utilisées dans chaque cas. Pour faciliter les interactions entre domaines, ces mesures de sécurité peuvent être considérées comme constituant une classe fonctionnelle particulière.

I.1.2 Utilisation de classes fonctionnelles au sein d'un même domaine

L'utilisation de classes fonctionnelles au sein d'un même domaine peut faciliter la définition de la sécurité. Les classes fonctionnelles peuvent également être utilisées à des fins de garantie de la sécurité. Les classes fonctionnelles doivent être associées, à cet effet, à un niveau de garantie déclaré par le fournisseur de produits de gestion. Ce point est en relation étroite avec des critères d'évaluation formelle.

Il peut être possible qu'un opérateur ait besoin de l'application d'une classe fonctionnelle particulière dans le cas d'une interaction avec le domaine d'un autre opérateur. Une raison éventuelle peut être l'impossibilité de traiter d'une manière efficace toutes les menaces au niveau de l'interface entre les deux domaines. Une solution possible serait d'assurer un niveau minimal de sécurité interne pour les deux RGT qui interagissent. Une norme de sécurité du RGT ne doit pas prescrire que des classes fonctionnelles sont requises, mais doit fournir la possibilité d'exiger certaines classes fonctionnelles en définissant des éléments de choix adéquats.

I.2 Classes fonctionnelles

Les classes fonctionnelles sont utilisées afin de définir de manière concise des groupes de services de sécurité qui ont pour but de fournir un certain niveau de sécurité. Le présent paragraphe présente à titre d'exemple un ensemble de classes fonctionnelles en indiquant de quelle manière ces dernières sont définies. Les classes fonctionnelles suivantes ont été proposées pour trois niveaux de sécurité de *l'interface X*:

1) Classe fonctionnelle minimale (FC 1).
2) Classe fonctionnelle de base (FC 2).
3) Classe fonctionnelle évoluée (FC 3).

Le nombre de classes fonctionnelles ne doit pas être trop élevé dans la pratique, mais il doit également être possible de satisfaire aux besoins de nombreux organismes différents. Les classes fonctionnelles peuvent être modifiées de la manière suivante:

– les classes fonctionnelles qui ont été définies uniquement pour l'interface X peuvent englober également les interfaces Q;

– on suppose que la confidentialité est une fonctionnalité optionnelle de toutes les classes pour les raisons suivantes:
  - il s'agit d'une prescription moins stricte;
  - l'inclusion obligatoire d'une classe fonctionnelle peut avoir des implications légales pour la possibilité d'utilisation de cette classe.

Le Tableau I.1 fournit un aperçu général des classes fonctionnelles proposées.

Tableau I.1/M.3016.0 – Classes fonctionnelles de services de sécurité

FC 1	FC 2	FC 3
Accent mis sur l'intégrité des ressources gérées stockées	FC 1 plus intégrité des données transférées	FC 2 plus responsabilité des opérations de gestion
• Authentification (entité homologue et utilisateur) • Contrôle d'accès à une association de gestion • Contrôle d'accès à une ressource gérée • Alarme de sécurité, audit et rétablissement	• Authentification (entité homologue et utilisateur) • Contrôle d'accès à une association de gestion • Contrôle d'accès à une ressource gérée • Authentification de l'origine des données • Intégrité sélective de champ • Intégrité de la connexion • Alarme de sécurité, audit et rétablissement	• Authentification (entité homologue et utilisateur) • Contrôle d'accès à une association de gestion • Contrôle d'accès à une ressource gérée • Authentification de l'origine des données • Intégrité sélective de champ • Intégrité de la connexion • Non-répudiation par la source • Non-répudiation par la destination • Alarme de sécurité, audit et rétablissement
Optionnel: • Intégrité de la connexion • Confidentialité de la connexion	Optionnel: • Confidentialité de la connexion • Confidentialité sélective de champ	Optionnel: • Confidentialité de la connexion • Confidentialité sélective de champ

Il est nécessaire de faire en outre la distinction entre les classes fonctionnelles s'appliquant au cas interdomaine et les classes fonctionnelles s'appliquant au cas intradomaine. Les prescriptions seront différentes dans chaque cas et les mesures de sécurité peuvent donc être différentes.

Il sera présenté dans ce qui suit un aperçu général portant sur des cas divers qui permettent au lecteur de découvrir quelles sont les classes fonctionnelles nécessaires et pertinentes.

Hypothèse

Il existe pour chaque domaine une autorité qui a la responsabilité de décider quelles sont les mesures à appliquer au sein de ce domaine.

On distingue les trois cas suivants:

1) classes fonctionnelles définies par une autorité de domaine s'appliquant au domaine en question (classe intradomaine);
2) classes fonctionnelles définies par une autorité de domaine s'appliquant aux interactions entre domaines (classe interdomaine). Ces classes fonctionnelles résulteront d'un accord entre les autorités des domaines qui interagissent;

3) classes fonctionnelles définies par une autorité de domaine s'appliquant aux prescriptions de sécurité interne d'un autre domaine.

Il est possible d'identifier dans chaque cas le nombre de classes fonctionnelles pour divers niveaux de sécurité.

Le nombre de niveaux de sécurité appelle une étude ultérieure.

L'ensemble de mesures de sécurité qui constitue une classe fonctionnelle appelle une étude ultérieure.

Les classes fonctionnelles des différents cas peuvent être identiques, ce qui réduit leur nombre total.

On peut également prendre en considération un compromis entre différents cas, par exemple si la sécurité interdomaine se trouve à un niveau élevé, les prescriptions de sécurité de l'autre domaine peuvent alors être moins strictes et réciproquement. Une autre possibilité est celle d'une classe fonctionnelle représentant un niveau de sécurité minimal pouvant être étendu le cas échéant par des mesures de sécurité adéquates.

I.3 Profils de sécurité

Les classes fonctionnelles ne nécessitent pas l'utilisation de mécanismes de sécurité normalisés, tout mécanisme satisfaisant aux prescriptions pouvant être utilisé.

L'interaction entre mesures de sécurité de domaines différents nécessite la conformité à des normes. Une prescription d'utilisation de normes particulières dont l'ensemble constitue une classe 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	**Gestion des télécommunications y compris le RGT et maintenance des réseaux**
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, communication entre systèmes ouverts et sécurité
Série Y	Infrastructure mondiale de l'information, protocole Internet et réseaux de prochaine génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2005