Union internationale des télécommunications

Sécurité dans les télécommunications et les technologies de l'information

Aperçu des problèmes et présentation des Recommandations UIT-T existantes sur la sécurité dans les télécommunications

Décembre 2003

UIT-T Secteur de la normalisation des télécommunications de l'UIT

Union internationale des télécommunications

Sécurité dans les télécommunications et les technologies de l'information

Aperçu des problèmes et présentation des Recommandations UIT-T existantes sur la sécurité dans les télécommunications

Remerciements

De nombreuses personnes ont participé à la préparation de ce Manuel, en contribuant à l'élaboration de Recommandations UIT-T pertinentes ou en participant à des réunions des Commissions d'études de l'UIT-T, à des ateliers ou à des séminaires. Il convient en particulier de remercier les personnes dont les noms ou les contributions sont cités ci-après. Mme Lakshmi Raman a rédigé le paragraphe 6.4 et une partie du paragraphe 2. Ce paragraphe a par ailleurs été revu par M. Herbert Bertine et M. Rao Vasireddy. Le paragraphe 3 sur les menaces et les risques découle de travaux réalisés par l'UIT-T ainsi que de la présentation figurant dans le document [Shannon]. Les paragraphes 5 et 6.5 sont fondés sur des informations générales tirées du document [Wisekey] et sur une aimable contribution de M. David Chadwick, notamment pour la description de l'application du paragraphe 6.5.2 concernant le système d'ordonnances médicales électroniques de Salford (ainsi que sur des passages tirés du document [Policy]). Le paragraphe 6.1 sur la téléphonie IP et les systèmes UIT-T H.323 a été établi à partir des documents [Packetizer] et [Euchner] ainsi que d'une aimable contribution de M. Martin Euchner. Le paragraphe 6.2 est fondé sur la Recommandation UIT-T J.169, le paragraphe 6.2.1 ayant été revu par M. Eric Rosenfeld. Le paragraphe 6.3 découle des Recommandations UIT-T T.30 et T.36. Les nombreux relecteurs anonymes sont également remerciés chaleureusement. L'Annexe C a été établie grâce à la contribution de nombreux experts des différentes Commissions d'études de l'UIT-T qui ont répondu au Questionnaire de la CE 17 de l'UIT-T sur la sécurité. Enfin, l'Annexe B a été élaborée à partir du catalogue des Recommandations relatives à la sécurité tenu à jour par des experts chargés d'étudier la Question 10/17 de l'UIT-T, notamment M. Sándor Mazgon.

Table des matières

Page

Page

Préface

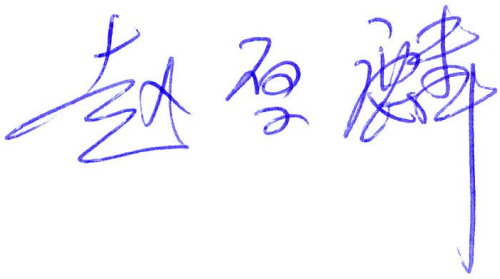
Autrefois restreinte à des domaines spécialisés tels que les applications bancaires, aérospatiales ou militaires, la sécurité numérique devient lentement mais sûrement l'affaire de tous.

L'ampleur prise par la sécurité numérique peut être attribuée à des événements importants tels que la dissémination de virus par courrier électronique ou le piratage d'informations concernant les cartes de crédit. Mais ce n'est pas tout. Les ordinateurs et les réseaux font maintenant partie de la vie quotidienne, au même titre que l'eau et l'électricité, de sorte que la sécurité numérique n'est plus un domaine réservé uniquement aux experts, les pouvoirs publics, les entreprises et les consommateurs s'y intéressent de plus en plus. Et puisque ordinateurs et réseaux envahissent autant notre vie professionnelle et notre vie privée, il est impératif que le fonctionnement de ces systèmes soit sécurisé.

Il est également primordial que le processus de sécurité soit bien conçu depuis la définition et la conception des systèmes, leur implémentation et jusqu'aux politiques et pratiques de déploiement, de mise en service et d'utilisation des systèmes. Lors de l'élaboration de normes, la sécurité doit toujours être prise en considération au cours des premières phases – et non ultérieurement – car c'est à ce moment que les vulnérabilités apparaissent. Le rôle des comités de normalisation est de se tenir au courant des problèmes connus au niveau des produits commercialisés et de les documenter, de proposer des solutions s'ils le peuvent et de publier des spécifications ou des lignes directrices visant à aider les implémenteurs et les utilisateurs à rendre les systèmes et services de communication suffisamment fiables.

L'UIT-T s'intéresse depuis de nombreuses années à la sécurité dans les télécommunications et les technologies de l'information. Toutefois, il n'est peut-être pas toujours facile de déterminer quels sujets ont été traités et dans quels documents ils l'ont été. Le présent manuel vise à rassembler, pour la première fois, toutes les informations disponibles. J'exprime toute ma gratitude aux ingénieurs du Bureau de la normalisation des télécommunications de l'UIT qui, conjointement avec divers experts provenant d'Etats Membres de l'UIT, ont réalisé la plus grande partie de cette tâche ardue. Le manuel est destiné à guider les techniciens, les cadres intermédiaires ainsi que les organes de réglementation dans la mise en œuvre pratique des fonctions de sécurité. A travers plusieurs exemples d'applications, les problèmes de sécurité sont expliqués, l'accent étant mis sur la manière dont ils sont pris en considération dans les Recommandations de l'UIT-T.

Je suis certain que ce manuel sera utile à tous ceux qui s'intéressent à la sécurité et j'invite les lecteurs à me communiquer leurs appréciations en vue des éditions futures.



Houlin Zhao

Directeur du Bureau de la normalisation des télécommunications

UIT

Genève, décembre 2003

Résumé

Le secteur des télécommunications, qui répond aux besoins d'un environnement commercial s'étendant de plus en plus à toute la planète, a permis d'améliorer la productivité et de mettre en relation des communautés dans le monde entier dans presque tous les secteurs industriels. Le fait que cette infrastructure de télécommunications soit si efficace résulte en grande partie des normes élaborées par des organismes tels que l'UIT-T. Les normes permettent non seulement de maintenir l'efficacité des réseaux actuels mais aussi de jeter les bases des réseaux des prochaines générations. Toutefois, tandis que les normes continuent de répondre aux besoins des utilisateurs finals et de l'industrie, l'utilisation croissante d'interfaces et de protocoles ouverts, la multiplicité des nouveaux acteurs, la diversité même des applications et des plates-formes et le fait que les implémentations ne sont pas toujours suffisamment testées ont augmenté les risques d'utilisation malveillante des réseaux. Ces dernières années, on a observé une forte augmentation des violations de la sécurité (virus et atteintes à la confidentialité de données enregistrées par exemple) dans les réseaux mondiaux, qui ont souvent entraîné de graves conséquences économiques. La question est alors de savoir comment prendre en charge une infrastructure de télécommunication ouverte sans compromettre les informations échangées sur cette infrastructure. La réponse est donnée par les efforts que les groupes de normalisation déploient pour élaborer des dispositions visant à combattre les menaces de sécurité dans tous les domaines de l'infrastructure des télécommunications, depuis les spécifications de protocole et les applications jusqu'à la gestion des réseaux. Ce manuel sur la sécurité vise à présenter et à offrir un aperçu global des nombreuses Recommandations élaborées par l'UIT-T – parfois en collaboration avec d'autres organismes de normalisation – en vue de sécuriser l'infrastructure des télécommunications ainsi que les services et applications associés.

Pour aborder les multiples aspects de la sécurité, il faut établir un cadre et une architecture afin de définir un vocabulaire commun qui servira de base à l'examen des concepts.

Le paragraphe 2 présente les éléments architecturaux définis dans la Recommandation UIT-T X.805 ainsi que les huit dimensions de sécurité qui ont été définies afin d'assurer la sécurité de bout en bout des applications de réseau – respect de la vie privée, confidentialité des données, authentification, intégrité, non-répudiation, contrôle d'accès, sécurité des communications et disponibilité. Ces principes généraux servent de base aux autres paragraphes et permettent d'en comprendre les détails. Les principaux éléments sont les couches de sécurité, les plans de sécurité et les dimensions appliquées à la combinaison de n'importe quelle couche et de n'importe quel plan.

Le paragraphe 3 définit trois termes essentiels employés à propos de la sécurité: vulnérabilité, menace et risque. Il décrit les caractéristiques distinctives des trois termes et donne quelques exemples. Il précise notamment comment vulnérabilité et menace se combinent pour créer un risque de sécurité.

Le paragraphe 4 s'appuie sur les informations données dans les paragraphes précédents pour définir des métaprescriptions relatives à l'établissement d'un cadre de sécurité. Les éléments essentiels permettant d'assurer une certaine sécurité et ainsi de combattre les menaces consistent à définir des mécanismes et algorithmes associés aux mesures de sécurité telles que l'authentification, le contrôle d'accès et le chiffrement des données. Le paragraphe 5 définit ces mécanismes au moyen des concepts d'infrastructure de clé publique et d'infrastructure de gestion de privilège. Ces mécanismes et infrastructures peuvent s'appliquer à bon nombre d'applications d'utilisateur final différentes.

Outre ce cadre, cette architecture et ces mécanismes, l'UIT-T a élaboré des dispositions relatives à la sécurité de plusieurs systèmes et services définis dans ses Recommandations. Une grande partie de ce manuel – le paragraphe 6 – porte donc sur des applications. Parmi les applications présentées dans cette première édition, figurent la téléphonie et les applications multimédias sur IP (H.323 et IPCablecom), la télésanté et la télécopie. Pour ces applications, on décrit l'architecture de déploiement et la manière dont les protocoles ont été définis pour répondre aux besoins de sécurité. Il faut non seulement offrir une sécurité des informations relatives aux applications, mais aussi sécuriser l'infrastructure du réseau et la gestion des services de réseau. Le paragraphe 6 contient donc aussi des exemples de normes dans lesquelles figurent des dispositions de sécurité relatives à la gestion de réseau.

De plus, cette version du manuel contient une liste d'acronymes et de définitions liés à la sécurité et à d'autres thèmes abordés dans ce document, extraits de Recommandations de l'UIT-T et d'autres sources (telles que la base de données SANCHO de l'UIT-T et le recueil de définitions relatives à la sécurité des systèmes de communication élaboré par la Commission d'études 17 de l'UIT-T). Cette liste figure en Annexe A. Ce manuel contient aussi la version actuelle du catalogue des Recommandations de l'UIT-T incluant des aspects de sécurité – la liste donnée en Annexe B est longue, ce qui est à l'image de l'étendue des travaux de l'UIT-T sur la sécurité. L'Annexe C résume les tâches liées à la sécurité auxquelles chacune des Commissions d'études de l'UIT-T est attelée. Les informations contenues dans ces Annexes sont constamment mises à jour et figurent à l'adresse www.itu.int/ITU-T.

En conclusion, l'UIT-T agit par anticipation, non seulement en ce qui concerne les technologies fondées sur IP mais aussi pour ce qui est de répondre aux besoins de nombreux secteurs industriels différents, dans lesquels les exigences de sécurité sont très variables. Ce manuel montre que les Recommandations de l'UIT-T offrent des solutions non seulement en termes de cadre et d'architecture génériques mais aussi pour des systèmes et des applications spécifiques, qui sont déjà déployés à l'échelle mondiale par des fournisseurs de réseaux et de services.

1 Domaine d'application du Manuel

Ce manuel donne un aperçu de la sécurité dans les télécommunications et dans les technologies de l'information, décrit des problèmes pratiques et indique comment l'UIT-T aborde les différents aspects de la sécurité dans les applications actuelles. Il a une portée didactique: il rassemble en un même endroit les informations relatives à la sécurité contenues dans les Recommandations de l'UIT-T et explique les relations respectives. Dans cette première édition, le manuel ne porte pas sur tous les aspects de la sécurité; en particulier, il ne traite ni des aspects qui se rapportent à la disponibilité, pour lesquels l'UIT-T a beaucoup à offrir, ni des dommages causés par l'environnement, domaine dans lequel l'UIT-T travaille également. Par ailleurs, les aspects traités sont fondés sur les travaux déjà réalisés, et non pas sur les travaux en cours, qui feront l'objet dans de futures éditions de ce manuel.

Ce manuel est destiné aux ingénieurs et aux chefs de produit, aux étudiants et au monde universitaire ainsi qu'aux organes de réglementation qui souhaitent mieux comprendre les problèmes de sécurité dans les applications pratiques.

2 Architecture et dimensions de sécurité fondamentales

La Recommandation X.805 définit le cadre de l'architecture et les dimensions permettant d'assurer la sécurité de bout en bout des applications réparties. Les principes généraux et les définitions s'appliquent à toutes les applications, même si les détails tels que les menaces et les vulnérabilités ainsi que les mesures visant à les contrer ou à les empêcher varient en fonction des besoins de chaque application.

L'architecture de sécurité est définie sur la base de deux principaux concepts: les couches et les plans. Les couches de sécurité se rapportent aux prescriptions qui s'appliquent aux éléments de réseau et aux systèmes qui constituent le réseau de bout en bout. On adopte une approche hiérarchique de subdivision des prescriptions entre les couches de manière à assurer la sécurité de bout en bout, couche après couche. Les trois couches sont les suivantes: la couche infrastructure, la couche services et la couche applications. La définition de couches présente notamment pour avantage de pouvoir réutiliser ces couches dans différentes applications pour assurer la sécurité de bout en bout. Les vulnérabilités au niveau de chaque couche sont différentes et il faut donc définir différentes contre-mesures pour répondre aux besoins de chaque couche. La couche infrastructure comprend les installations de transmission de réseau et les différents éléments de réseau. Elle comprend notamment les routeurs, commutateurs et serveurs ainsi que les liaisons de communication qui les relient. La couche services concerne la sécurité des services de réseau qui sont offerts aux clients. Ces services vont des offres de connexion de base telles que les services de lignes louées aux services à valeur ajoutée tels que la messagerie instantanée. La couche applications concerne les prescriptions relatives aux applications de réseau utilisées par les clients. Ces applications peuvent être aussi simples que la messagerie électronique ou aussi complexes que la visualisation collaborative, pour laquelle des transferts vidéo très haut de gamme sont opérés dans les domaines de l'exploration pétrolière, de la conception d'automobiles, etc.

Le second axe du cadre concerne la sécurité des activités exécutées dans un réseau. Le cadre de sécurité définit trois plans de sécurité pour représenter les trois types d'activités protégées qui ont lieu dans un réseau. Les plans de sécurité sont les suivants: (1) le plan de gestion, (2) le plan de commande et (3) le plan d'utilisateur final. Ils visent à répondre aux besoins de sécurité particuliers associés aux activités de gestion de réseau, aux activités de signalisation et de commande de réseau et aux activités d'utilisateur final correspondantes. Le plan de gestion, examiné plus en détail au § 6.4, se rapporte aux activités d'exploitation, d'administration, de maintenance et de configuration (OAM&P), par exemple la configuration d'un utilisateur ou d'un réseau, etc. Le plan de commande est associé aux aspects de signalisation pour l'établissement (et la modification) de la communication de bout en bout dans le réseau, quel que soit le support et la technologie utilisés dans le réseau. Le plan d'utilisateur final concerne la sécurité d'accès au réseau et d'utilisation du réseau par les clients. Il se rapporte aussi à la protection des flux de données d'utilisateur final.

Outre les couches de sécurité et les plans de sécurité constituant les deux axes (3 plans de sécurité et 3 couches de sécurité), le cadre définit aussi huit dimensions concernant la sécurité de réseau. Ces dimensions sont définies dans les paragraphes qui suivent. D'un point de vue architectural, ces dimensions sont appliquées à chaque cellule de la matrice 3x3 formée par les couches et les plans de manière à pouvoir déterminer les contre-mesures appropriées. La Figure 1 illustre les plans, couches et dimensions de sécurité de l'architecture de sécurité. Le § 6.4 portant sur le plan de gestion montre comment les trois cellules de la matrice 3x3 relatives au plan de gestion sont prises en considération dans les autres Recommandations de l'UIT-T.

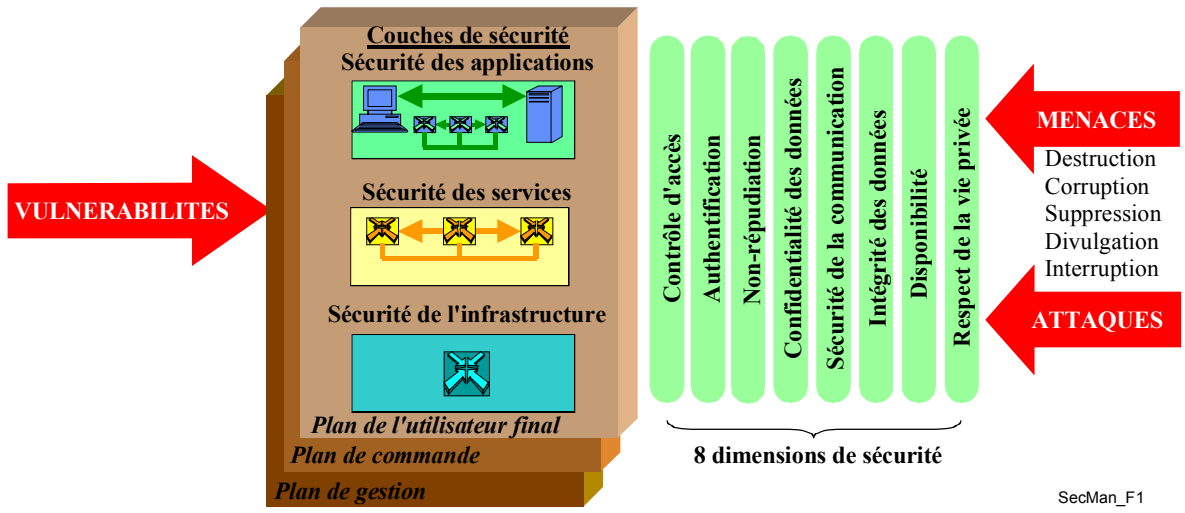


Figure 1
Eléments architecturaux de sécurité (Recommandation UIT-T X.805)

2.1 Respect de la vie privée et confidentialité des données

Le concept de respect de la vie privée constitue une motivation fondamentale en matière de sécurité. Par respect de la vie privée, on entend généralement le droit des individus de contrôler ou d'agir sur les informations les concernant qui peuvent être collectées et stockées ainsi que sur les personnes par lesquelles et auxquelles ces informations peuvent être divulguées. Par extension, le respect de la vie privée est en outre associé à certains moyens techniques (par exemple la cryptographie) visant à garantir que ces informations ne sont divulguées qu'aux personnes voulues et ce, afin que seules les parties explicitement autorisées puissent interpréter le contenu échangé entre elles.

Plus couramment, respect de la vie privée et confidentialité sont utilisés comme synonymes mais il convient de noter que la Recommandation UIT-T X.805 fait une distinction entre ces deux termes, le respect de la vie privée se rapportant à la protection de l'association entre l'identité des utilisateurs et les activités qu'ils exécutent (habitudes d'achats en ligne, sites Internet visités, etc.) et la confidentialité des données se rapportant à la protection contre tout accès non autorisé à des contenus de données. Le chiffrement, les listes de contrôle d'accès et les permissions d'accès aux fichiers sont des méthodes souvent utilisées pour assurer la confidentialité des données.

Le terme respect de la vie privée apparaît dans plusieurs Recommandations de l'UIT-T, notamment F.115, H.235, J.160, Q.1531, X.800 et X.805.

2.2 Authentification

L'authentification consiste à prouver que l'identité déclarée par une entité est bien la sienne. Les entités désignent ici non seulement les utilisateurs humains mais aussi les dispositifs, les services et les applications. L'authentification permet par ailleurs de garantir qu'une entité ne tente pas d'usurper l'identité d'une autre entité ou de relancer une communication précédente sans y être autorisée. Il existe deux types d'authentification: l'authentification de l'origine des données (c'est-à-dire l'authentification demandée dans une association en mode connexion) et l'authentification de l'entité homologue (c'est-à-dire l'authentification dans une association en mode sans connexion). Le réseau doit faire en sorte qu'un échange de données soit établi avec l'entité homologue voulue (et non avec une entité tentant de se faire passer pour l'entité voulue ou de relancer une communication précédente) et que l'origine des données corresponde à l'origine déclarée. L'authentification suit généralement l'identification. Les informations utilisées pour l'identification, l'authentification et l'autorisation doivent être protégées par le réseau.

Le terme authentification apparaît dans plusieurs Recommandations de l'UIT-T, notamment F.500, F.851, F.852, H.235, J.160, J.93, J.95, M.60, X.217, X.217-Bis, X.509, X.800, X.805 et X.811.

2.3 Intégrité

L'intégrité des données signifie que les données n'ont pas été modifiées de manière non autorisée. Par extension, l'intégrité des données garantit aussi la protection des informations contre les modifications, suppressions, créations et duplications non autorisées et signale ces activités non autorisées.

Le terme intégrité apparaît dans plusieurs Recommandations de l'UIT-T, notamment H.235, J.160, J.93, J.95, Q.1290, Q.1531, X.800 et X.815.

2.4 Non-répudiation

La non-répudiation est la capacité d'empêcher les utilisateurs de nier ultérieurement qu'ils ont exécuté une action. Ces actions comprennent la création, l'envoi, la réception et la remise de contenu (par exemple envoi ou réception de messages, établissement ou réception d'appels, participation à des conférences audio et vidéo, etc.).

La non-répudiation permet de fournir une preuve irréfutable de l'envoi et/ou de la réception de données afin d'empêcher l'expéditeur de désavouer un message légitime ou le destinataire de nier la réception d'un message. Le réseau peut prendre en charge l'une des deux formes suivantes ou les deux: le destinataire des données reçoit une preuve de l'origine des données, ainsi l'expéditeur ne pourra pas nier avoir envoyé les données ou leur contenu; ou l'expéditeur reçoit une preuve de la remise des données, ainsi le destinataire ne pourra pas nier avoir reçu les données ou leur contenu.

Le terme non-répudiation apparaît dans plusieurs Recommandations de l'UIT-T, notamment F.400, F.435, F.440, J.160, J.93, J.95, M.60, T.411, X.400, X.805, X.813 et X.843.

2.5 Autres dimensions définies dans la Recommandation X.805

En plus du respect de la vie privée et de la confidentialité des données, de l'authentification, de l'intégrité et de la non-répudiation, la Recommandation UIT-T X.805 définit les trois autres dimensions de sécurité suivantes: contrôle d'accès, communication et disponibilité.

La dimension de sécurité *contrôle d'accès* assure la protection contre toute utilisation non autorisée de ressources de réseau. Le contrôle d'accès garantit que seuls les personnes ou les dispositifs autorisés peuvent accéder aux éléments de réseau, aux informations stockées, aux flux d'information, aux services et aux applications. Il est défini au § 6.3 de la Recommandation UIT-T X.810 et dans la Recommandation UIT-T X.812. Le contrôle d'accès et l'authentification sont liés mais ont des portées différentes.

La dimension de sécurité *communication* est une nouvelle dimension définie dans la Recommandation UIT-T X.805 qui garantit que les informations ne circulent qu'entre les points d'extrémité autorisés. Cette dimension se rapporte aux mesures visant à contrôler les flux de trafic dans le réseau afin d'empêcher les déroutements et interceptions de trafic.

La dimension de sécurité *disponibilité* garantit que l'accès autorisé aux éléments de réseau, aux informations stockées, aux flux d'information, aux services et aux applications n'est pas refusé par suite d'une coupure du réseau. Les solutions de rétablissement de réseau et de retour à la normale après une catastrophe font partie de cette catégorie.

3 Vulnérabilités, menaces et risques

Cherchant à tout prix à implémenter la solution IT la plus avantageuse ou à déterminer, parmi les applications web, les serveurs et les bases de données les plus récents et les plus attrayants, celui qui répond le mieux à leurs objectifs, les organisations ont souvent relégué au second plan la protection des informations contenues dans ces ressources. De nombreuses entreprises risquent d'être dupées si elles pensent qu'étant donné qu'elles n'ont pas été touchées, il n'existe pas de menace.

Les organismes de normalisation ont une capacité et une responsabilité uniques pour ce qui est d'aborder les vulnérabilités de sécurité dans les protocoles. Il existe des mesures immédiates et relativement simples que ces organismes peuvent prendre pour améliorer la sécurité de tous les protocoles en cours de normalisation.

Une *vulnérabilité de sécurité* est un défaut ou une faiblesse dans la conception, l'implémentation ou l'exploitation d'un système, susceptible d'être exploité à des fins de violation de sécurité du système (RFC 2828). Ce n'est ni un risque, ni une menace, ni une attaque.

Les vulnérabilités peuvent être de quatre types. Les vulnérabilités du *modèle des menaces* proviennent de la difficulté à prévoir des menaces futures (par exemple système de signalisation N° 7). Les vulnérabilités de *conception et spécification* proviennent d'erreurs ou d'oublis dans la conception d'un protocole qui le rendent intrinsèquement vulnérable (par exemple WEP dans IEEE 802.11b alias WiFi). Les vulnérabilités d'*implémentation* sont des vulnérabilités qui découlent d'erreurs dans l'implémentation d'un protocole. Enfin, les vulnérabilités d'*exploitation et de configuration* proviennent d'un mauvais usage d'options dans des implémentations ou de politiques de déploiement déficientes (par exemple la non-obligation d'utiliser le chiffrement dans un réseau WiFi ou le choix par un administrateur de réseau d'un mauvais chiffrement continu).

Conformément à la Recommandation X.800, une *menace de sécurité* est une violation potentielle de la sécurité, qui peut être active (menace de modification non autorisée et délibérée de l'état d'un système) ou passive (menace de divulgation non autorisée d'informations sans que l'état du système ne soit modifié). L'usurpation de l'identité d'une entité autorisée et le déni de service sont des exemples de menaces actives et l'écoute clandestine pour voler un mot de passe en clair est un exemple de menace passive. Les agents de menaces peuvent être des pirates, des terroristes, des vandales, le crime organisé ou des agents soutenus par un Etat, mais dans un très grand nombre de cas, les menaces proviennent de personnes en place dans une organisation.

Un *risque de sécurité* apparaît lorsqu'une vulnérabilité de sécurité est combinée avec une menace de sécurité. Par exemple, un bogue au niveau du débordement dans une application de système d'exploitation (c'est-à-dire une vulnérabilité) associé à la connaissance, aux outils appropriés et à l'accès d'un pirate (c'est-à-dire une menace) peuvent entraîner un risque d'attaque de serveur web. Les risques de sécurité peuvent avoir pour conséquences une perte de données, une corruption de données, une atteinte au respect de la vie privée, une fraude, un temps d'arrêt ou une perte de la confiance du public.

Les menaces de sécurité varient alors que les vulnérabilités de sécurité existent pendant toute la durée de vie d'un protocole. Avec les protocoles normalisés, les risques de sécurité fondés sur les protocoles peuvent être très élevés et concerner le monde entier, d'où l'importance de comprendre et d'identifier les vulnérabilités présentes dans les protocoles.

4 Nécessité d'un cadre de sécurité

Différentes entités ont besoin d'un cadre de sécurité de réseau générique:

- Les clients/abonnés veulent que le réseau et les services offerts soient fiables et que les services soient disponibles (notamment les services d'urgence) en cas de catastrophes majeures (y compris les actes terroristes).

- Les pouvoirs publics exigent que la sécurité fasse l'objet de directives et de lois, afin de garantir la disponibilité des services, une concurrence loyale et la protection du respect de la vie privée.

- Les opérateurs de réseau et les fournisseurs de service ont eux-mêmes besoin de sécurité pour sauvegarder leurs intérêts opérationnels et commerciaux et pour satisfaire à leurs obligations vis-à-vis des clients et du grand public.

Les exigences de sécurité pour les réseaux et services de télécommunication devraient de préférence s'appuyer sur des normes de sécurité adoptées à l'échelle internationale. En effet, cela permet d'accroître l'interopérabilité et évite de devoir faire deux fois le même travail et de devoir réinventer la roue. La mise en œuvre et l'utilisation de services et de mécanismes de sécurité peuvent s'avérer relativement onéreuses par rapport à la valeur des transactions protégées. Il faut trouver un compromis entre le coût des mesures de sécurité et les conséquences financières potentielles de violations de la sécurité. Il est donc important de pouvoir personnaliser la sécurité offerte en fonction des services à protéger. Pour cela, il convient d'offrir les services et mécanismes de sécurité sous une forme qui permette de procéder à cette personnalisation. En raison du grand nombre de combinaisons possibles des fonctions de sécurité, il est souhaitable de disposer de profils de sécurité qui s'adaptent à une grande variété de réseaux et services de télécommunication.

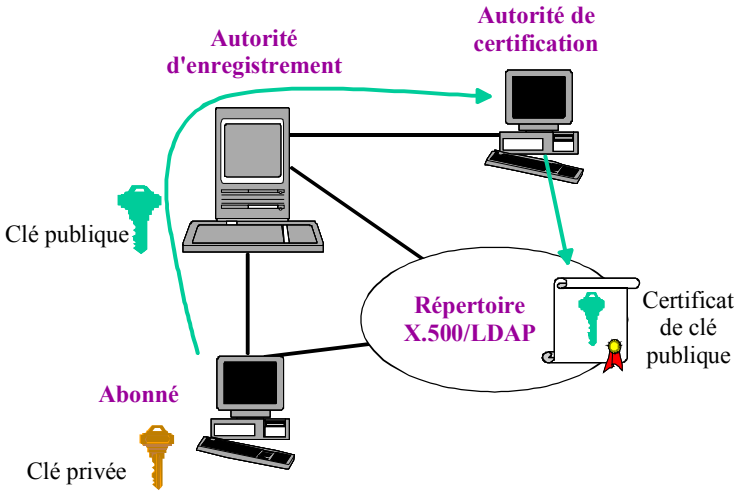
La normalisation facilite la réutilisation de solutions et de produits, ce qui signifie que la sécurité peut être mise en œuvre plus rapidement et à un moindre coût.

Les solutions normalisées présentent aussi de gros avantages pour les fabricants et les utilisateurs des systèmes: réalisation d'économies d'échelle lors de l'élaboration des produits et interfonctionnement des composants dans les réseaux de télécommunication du point de vue de la sécurité.

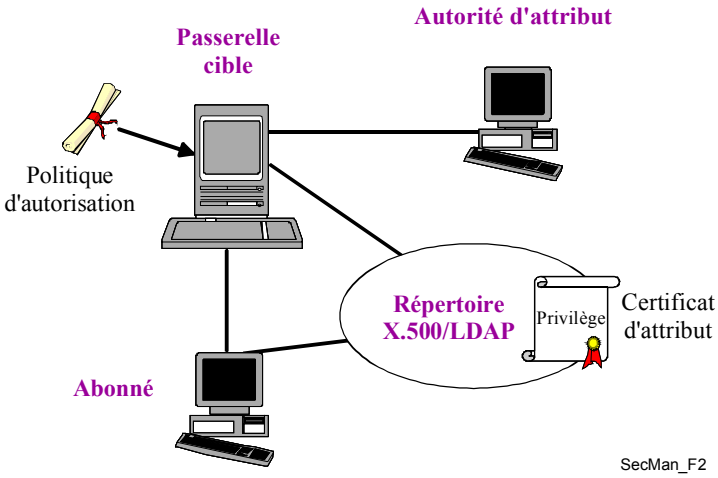
Les services et mécanismes de sécurité qui peuvent être offerts aux opérateurs de réseaux ou aux fournisseurs de services de télécommunication visent à assurer une protection contre les attaques malveillantes telles que le déni de service, l'écoute clandestine, la mystification, l'altération des messages (modification, retard, suppression, insertion, relecture, réacheminement, déroutement ou réordonnancement de messages), la répudiation ou la falsification. La protection comprend la prévention et la détection des attaques et le retour à la normale après une attaque, des mesures visant à empêcher les interruptions de service dues à des événements naturels (météorologiques, etc.) ainsi que la gestion des informations liées à la sécurité. Il faut convenir de dispositions qui permettent aux autorités légales dûment autorisées de procéder à des interceptions licites lorsqu'elles en font la demande.

5 Infrastructure PKI et gestion des privilèges avec la Recommandation X.509

L'infrastructure de clé publique (PKI, *public key infrastructure*) X.509 est une norme d'authentification forte, fondée sur des certificats de clé publique et des autorités de certification. Elle permet d'authentifier les messages des parties qui communiquent entre elles et ce, de façon modulable. La technologie fondamentale d'une infrastructure PKI est la cryptographie à clé publique, que l'on décrira donc en premier. En plus de l'infrastructure PKI, la Recommandation X.509 définit aussi une infrastructure de gestion de privilège (PMI, *privilege management infrastructure*), qui est une norme d'autorisation forte, fondée sur des certificats d'attribut et des autorités d'attribut. L'infrastructure PMI sert à vérifier les droits et privilèges des utilisateurs. Les composants des infrastructures PKI et PMI sont illustrés sur la Figure 2.



(a) Composants d'une infrastructure de clé publique



(b) Composants d'une infrastructure de gestion de privilège

Figure 2
Composantes des infrastructures PKI et PMI

5.1 Cryptographie à clé secrète et cryptographie à clé publique

Dans un système de cryptographie *symétrique* (ou *à clé secrète*), on utilise la même clé pour le chiffrement et pour le déchiffrement, comme illustré sur la Figure 3(a). Il faut donc faire en sorte que les individus puissent partager une clé secrète unique. La clé doit être distribuée aux individus par des moyens sécurisés, car la connaissance de la clé de chiffrement implique la connaissance de la clé de déchiffrement et inversement.

Un système de cryptographie *asymétrique* (ou à *clé publique*) fait intervenir deux clés, comme illustré sur la Figure 3(b) – une clé publique et une clé privée. La première est rendue publique alors que la seconde est gardée secrète. La clé publique est différente de la clé privée et, bien que ces clés soient liées mathématiquement, il n'existe pas de procédé connu permettant de déduire la clé privée de la clé publique. La clé publique est distribuée largement alors que la clé privée est gardée secrète (par exemple sur une carte à puce ou sur un jeton, ou également sur un assistant personnel ou sur un téléphone mobile dans le futur). D'une manière générale, pour envoyer des données confidentielles chiffrées, l'expéditeur chiffre les données avec la clé publique du destinataire et le destinataire les déchiffre avec sa clé privée correspondante. Pour envoyer des données authentifiées, l'expéditeur chiffre les données avec sa clé privée et le destinataire les authentifie avec la clé publique correspondante de l'expéditeur. Toutefois, le chiffrement asymétrique utilisé de cette façon présente deux inconvénients. Premièrement, le chiffrement à clé publique nécessite de très longs calculs, il est donc inefficace de chiffrer des messages entiers au moyen du chiffrement asymétrique. Deuxièmement, si la totalité du message est chiffrée, il est impossible d'acheminer les messages à leurs destinataires car les nœuds intermédiaires ne peuvent pas déterminer qui est le destinataire. Dans la pratique, le chiffrement asymétrique n'est donc utilisé que pour chiffrer de petites parties de messages. Lorsque la confidentialité est requise, le message est chiffré au moyen du chiffrement symétrique classique et la clé symétrique est soumise à un chiffrement asymétrique au moyen de la clé publique du destinataire. Lorsque l'authentification est requise, le message est haché au moyen d'une fonction de hachage unidirectionnelle sécurisée telle que SHA-1 ou MD-5 et la valeur de hachage résultante codée sur 160 ou 128 bits est soumise à un chiffrement asymétrique au moyen de la clé privée de l'expéditeur puis jointe au message (qui est envoyé en clair) avant le transfert. Ce total de contrôle cryptographique joint est appelé signature numérique – élément important pour le commerce électronique.

Pour le chiffrement à clé publique, chacun doit posséder les clés publiques correctes des propriétaires de clé privée respectifs. Si Bob croit à tort qu'il possède la clé publique d'Alice, alors qu'en réalité, la clé publique correspond à la clé privée de Jane, Bob croira que les messages signés numériquement par Jane viennent en fait d'Alice (ce qui permet à Jane d'usurper l'identité d'Alice). De plus, si Bob souhaite envoyer un message confidentiel à Alice, Jane pourra intercepter et déchiffrer ce message, tandis qu'Alice ne pourra pas le lire. Il est donc primordial que chacun puisse valider le propriétaire légitime d'une clé publique.

5.2 Certificats de clé publique

Un certificat de clé publique (parfois appelé "certificat numérique") est un moyen permettant de valider le propriétaire d'une paire de clés asymétriques. Un certificat de clé publique rattache fortement une clé publique au nom de son propriétaire et il est signé numériquement par l'autorité de confiance attestant ce rattachement. Cette autorité de confiance est appelée autorité de certification (CA, *certification authority*). Le format normalisé admis sur le plan international pour les certificats de clé publique est défini dans la norme X.509. Brièvement, un certificat de clé publique X.509 comprend une clé publique, un identificateur de l'algorithme asymétrique avec lequel la clé doit être utilisée, le nom du propriétaire de la paire de clés, le nom de l'autorité de certification attestant cette propriété, le numéro de série et la durée de validité du certificat, le numéro de la version X.509 à laquelle ce certificat est conforme et un ensemble facultatif de champs d'extension contenant des informations sur la politique de certification de l'autorité de certification. Le certificat entier est alors

signé numériquement au moyen de la clé privée de l'autorité de certification. Le certificat X.509 peut alors être publié largement, par exemple sur un site web, dans un annuaire LDAP ou sur la carte de visite électronique (vCard) attachée aux messages électroniques et la signature de l'autorité de certification garantit que le contenu du certificat ne peut pas être altéré sans que l'on s'en rende compte.

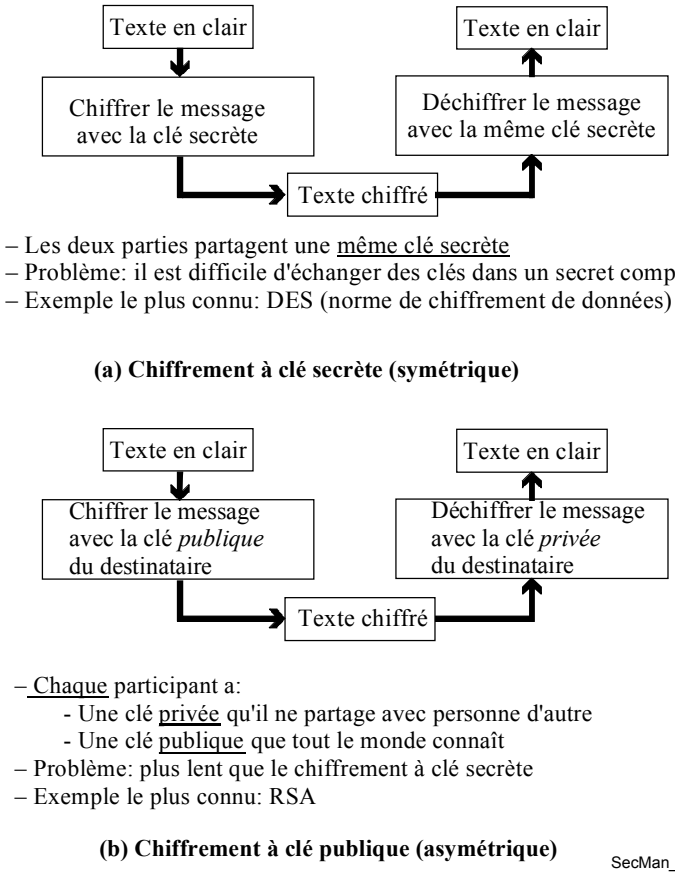


Figure 3
Illustration des processus de chiffrement symétrique (ou à clé privée) et asymétrique (ou à clé publique) et mise en évidence des particularités

Il est évident que pour pouvoir valider le certificat de clé publique d'un utilisateur, nous avons besoin de pouvoir accéder à la clé publique valable de l'autorité de certification qui a établi ce certificat, de manière à pouvoir vérifier la signature présente sur ce certificat. La clé publique d'une autorité ce certification peut être certifiée par une autre autorité de certification (supérieure), la validation des clés publiques devenant alors récursive à mesure que nous nous déplaçons le long de la chaîne de certificats. Au bout du compte, cette chaîne doit avoir une fin, qui correspond généralement au certificat autosigné de l'autorité de certification qui constitue notre "racine de confiance". Les clés publiques d'autorité de certification racine sont distribuées sous la forme de certificats autosignés (dans lesquels les autorités de certification racines attestent qu'il s'agit de leur propre clé publique). La signature nous permet alors de valider le fait que la clé et le nom de l'autorité de certification n'ont pas été altérés depuis la création du certificat. Toutefois, nous ne pouvons pas prendre pour argent comptant le nom de l'autorité de certification figurant dans un certificat autosigné, car c'est l'autorité de certification qui a inséré le nom dans le certificat. Il est donc essentiel dans une infrastructure de clé publique que les clés publiques d'autorité de certification racine (sous forme de certificats autosignés)

soient distribuées de manière sécurisée, afin que nous puissions être certains qu'une clé publique appartient réellement à l'autorité de certification racine dont le nom figure dans le certificat autosigné. Sans cela, nous ne pouvons pas être sûrs que l'identité de l'autorité de certification racine n'est pas usurpée.

5.3 Infrastructures de clé publique

L'infrastructure PKI est principalement destinée à émettre et gérer les certificats de clé publique, y compris les certificats autosignés d'autorité de certification racine. La gestion de clés comprend la création de paires de clés, la création de certificats de clé publique, la révocation de certificats de clé publique (par exemple si la clé privée d'un utilisateur a été compromise), le stockage et l'archivage des clés et des certificats et leur destruction une fois qu'ils sont arrivés au terme de leur vie. Chaque autorité de certification suit un ensemble de politiques et la norme X.509 définit des mécanismes permettant de distribuer (une partie de) ces informations de politique dans les champs d'extension des certificats X.509 émis par les autorités de certification. Les règles et procédures politiques suivies par une autorité de certification sont généralement définies dans une politique de certificat (CP, *certificate policy*) et dans une déclaration de pratique de certification (CPS, *certification practice statement*), qui sont des documents publiés par l'autorité de certification. Ces documents constituent une base de qualité commune nous permettant d'évaluer la confiance que nous pouvons avoir concernant les certificats de clé publique émis par les autorités de certification, à la fois sur le plan international et d'un secteur à l'autre. Ils donnent aussi (une partie du) le cadre juridique nécessaire à l'établissement d'une confiance interorganisations et à la spécification de restrictions quant à l'utilisation des certificats émis.

Il est à noter que, dans le cas de l'authentification fondée sur des certificats de clé publique, les points d'extrémité sont tenus de fournir des signatures numériques établies au moyen de la valeur de la clé privée associée. L'échange de certificats de clé publique seuls n'offre pas de protection contre les attaques par interposition (man-in-the-middle).

5.4 Infrastructure de gestion de privilège

La Recommandation UIT-T X.509 spécifiait dans ses premières versions les éléments de base des infrastructures de clé publique (PKI) et définissait notamment les certificats de clé publique. La révision approuvée en 2000 contient des précisions sur les certificats d'attribut et définit un cadre pour l'infrastructure de gestion de privilège. Les mécanismes définis permettent d'établir des privilèges d'accès pour les utilisateurs dans un environnement multifabricants et multi-applications.

Les infrastructures PMI et PKI utilisent des concepts analogues, mais la première concerne l'autorisation tandis que la seconde concerne l'authentification. La Figure 2 et le Tableau 1 illustrent les analogies entre les deux infrastructures.

Tableau 1
Comparaison des caractéristiques de l'infrastructure de gestion de privilège et de l'infrastructure de clé publique

Infrastructure de gestion de privilège	Infrastructure de clé publique
Source d'autorité (SoA)	Autorité de certification racine (point d'ancrage de confiance)
Autorité d'attribut (AA)	Autorité de certification
Certificat d'attribut	Certificat de clé publique
Liste de révocation de certificat d'attribut	Liste de révocation de certificat
Liste de révocation d'autorité pour l'infrastructure PMI	Liste de révocation d'autorité pour l'infrastructure PKI

L'attribution de privilèges aux utilisateurs vise à faire en sorte que les utilisateurs suivent une politique de sécurité prescrite établie par la source d'autorité. Les informations relatives à cette politique sont rattachées au nom d'utilisateur dans le certificat d'attribut et comprennent un certain nombre d'éléments illustrés sur la Figure 4.

Version
Détenteur
Emetteur
Signature (identificateur d'algorithme)
Numéro de série de certificat
Durée de validité
Attributs
Identificateur unique de l'émetteur
Extensions

Figure 4
Structure d'un certificat d'attribut X.509

Le modèle de contrôle d'infrastructure PMI défini dans la Recommandation UIT-T X.509 est constitué de cinq composants: le déclarant de privilège, le vérificateur de privilège, la méthode objet[1], la politique de privilège et les variables d'environnement (voir la Figure 5). Les procédés décrits permettent au vérificateur de privilège de contrôler l'accès du déclarant de privilège à la méthode objet, conformément à la politique de privilège.

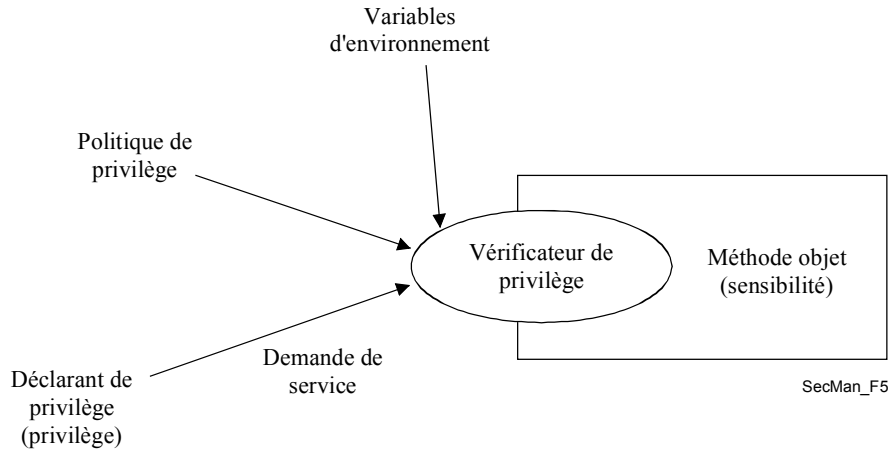


Figure 5
Modèle de contrôle de l'infrastructure PMI (Recommandation UIT-T X.509)

[1] Une méthode objet est définie comme une action qui peut être invoquée sur une ressource (par exemple un système de fichiers peut avoir des méthodes objets lecture, écriture et exécution).

Pour certaines implémentations, il peut être nécessaire de déléguer un privilège. La Recommandation UIT-T X.509 définit un modèle de délégation d'architecture PMI à quatre composants: le vérificateur de privilège, la source d'autorité, d'autres autorités d'attribut et le déclarant de privilège (voir la Figure 6).

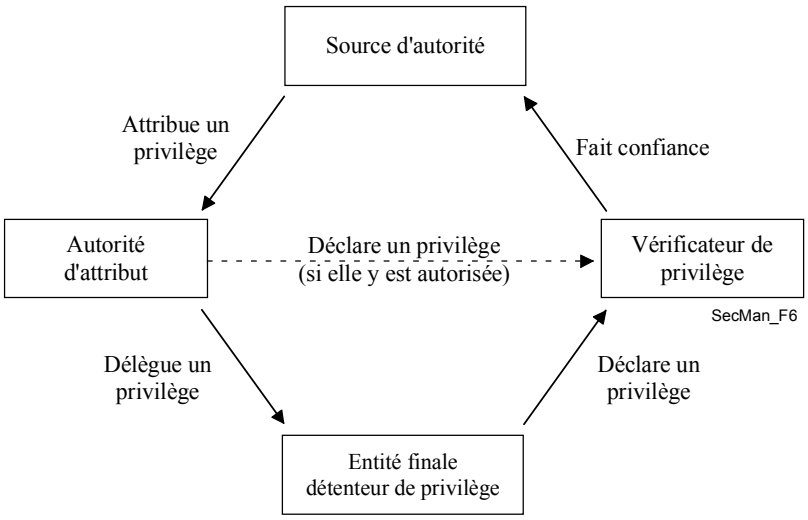


Figure 6
Modèle de délégation d'infrastructure PMI (Recommandation UIT-T X.509)

Dans les implémentations récentes de systèmes d'autorisation fondées sur le modèle du contrôle d'accès à base de rôle (RBAC, *role-based access control*), on considère qu'un rôle est attribué à l'utilisateur. La politique d'autorisation associe un ensemble de permissions à un rôle. Lorsque l'utilisateur accède à une ressource, son rôle est d'abord vérifié avant qu'il ne puisse invoquer des actions. Le système d'ordonnances électroniques décrit au 6.5.2 est un exemple d'utilisation d'un système RBAC.

6 Applications

Les applications dont il est question ici appartiennent à deux catégories distinctes. La première catégorie correspond aux applications d'utilisateur final. Elle comprend notamment la téléphonie IP, pour laquelle l'architecture de réseau et les composants utilisés pour offrir cette application d'utilisateur final sont décrits. Des problèmes de sécurité et des solutions sont examinés dans les trois plans de sécurité dans le cas des applications multimédias et de la VoIP en particulier. Le système IPCablecom, qui offre des services IP en temps réel sur un réseau de transmission par câble, et la transmission de télécopie sont deux autres applications d'utilisateur final traitées ici. Parmi les applications qui ne sont pas propres au secteur des télécommunications et qui sont examinées ici, figure la télésanté et notamment un système d'ordonnances électroniques. La seconde catégorie correspond aux applications de gestion de réseau, dans lesquelles, la sécurité est un élément important à prendre en considération afin que la qualité et l'intégrité des services offerts par les fournisseurs puissent être respectées. Il est donc impératif de mettre en place un système approprié de privilèges et d'autorisations pour l'exécution des activités de gestion.

6.1 Téléphonie IP utilisant des systèmes H.323

La téléphonie IP, également appelée voix sur IP (VoIP, *voice-over-IP*), désigne la fourniture de services traditionnellement offerts sur le RTPC à commutation de circuit sur un réseau utilisant le protocole IP (sur lequel l'Internet est également fondé). Ces services comprennent avant tout la téléphonie, avec les services complémentaires associés tels que la conférence téléphonique (par pont de conférence), le renvoi d'appel, l'appel en instance, les lignes multiples, la déviation d'appel, la mise en garde et l'interception d'appel, la consultation et la fonction suis-moi, et bien d'autres services de réseau intelligent, ainsi que les données en bande téléphonique dans certains cas. La téléphonie sur Internet est un cas particulier de VoIP, dans lequel le trafic téléphonique est acheminé sur l'Internet public.

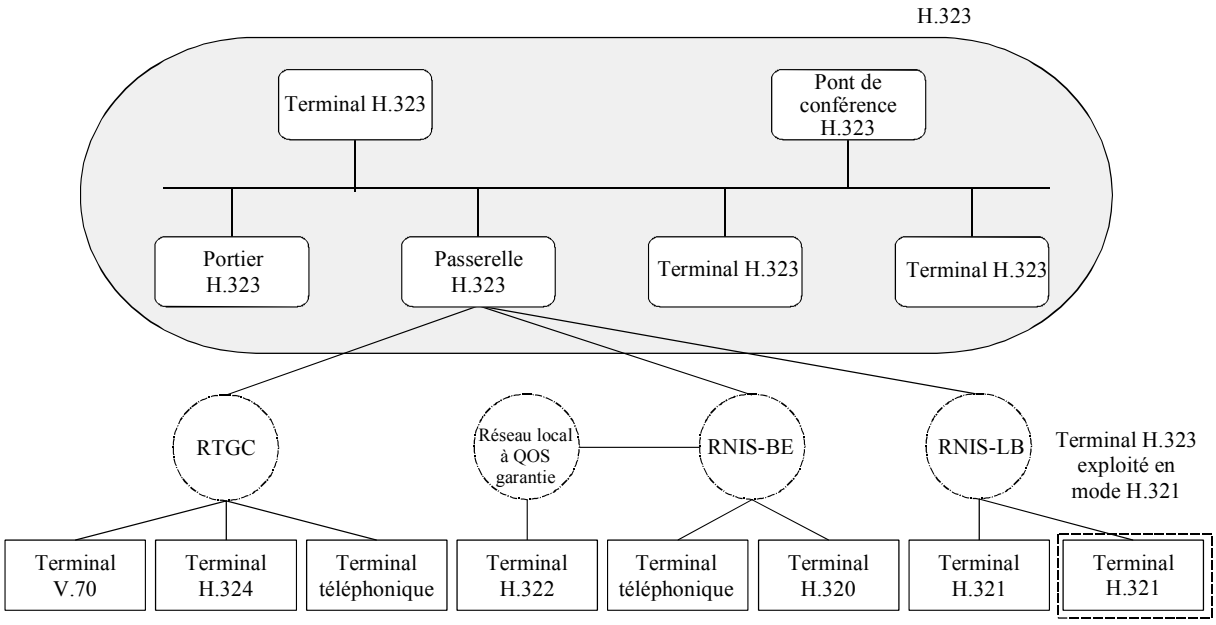
H.323 est une Recommandation cadre de l'UIT-T qui jette les bases des communications audio, vidéo et de données sur des réseaux locaux ou des réseaux IP, y compris l'Internet, qui n'offrent pas de qualité de service garantie. Ces réseaux, qui sont actuellement les principaux réseaux utilisés dans les entreprises, emploient les technologies de réseau suivantes: TCP/IP à commutation par paquet et IPX sur Ethernet, Fast Ethernet et Token Ring. Les produits et applications multimédias issus de différents fabricants mais conformes à la Recommandation H.323 peuvent interfonctionner, ce qui permet aux utilisateurs de communiquer sans avoir à se soucier de la compatibilité. Le protocole H.323 a été le premier protocole de téléphonie IP à être défini et il est considéré comme la pierre angulaire pour les produits de réseau local destinés aux applications d'abonné, de divertissement, commerciales et professionnelles. Les principales Recommandations concernant le système H.323 sont les suivantes:

- H.323 – document "cadre" qui décrit l'utilisation des Recommandations H.225.0 et H.245 et d'autres documents connexes pour la fourniture de services de conférence multimédias en mode paquet
- H.225.0 – document qui décrit trois protocoles de signalisation (RAS, signalisation d'appel et "Annexe G")
- H.245 – protocole de commande multimédia (commun aux Recommandations H.310, H.323 et H.324)
- H.235 – sécurité dans les systèmes de type H.245
- H.246 – interfonctionnement avec le RTPC
- H.450.x – services complémentaires
- H.460.x – diverses extensions du protocole H.323
- H.501 – protocole de gestion de la mobilité et communications intra et interdomaniales
- H.510 – mobilité d'utilisateur, de terminal et de service
- H.530 – spécification de la sécurité pour la Recommandation H.510

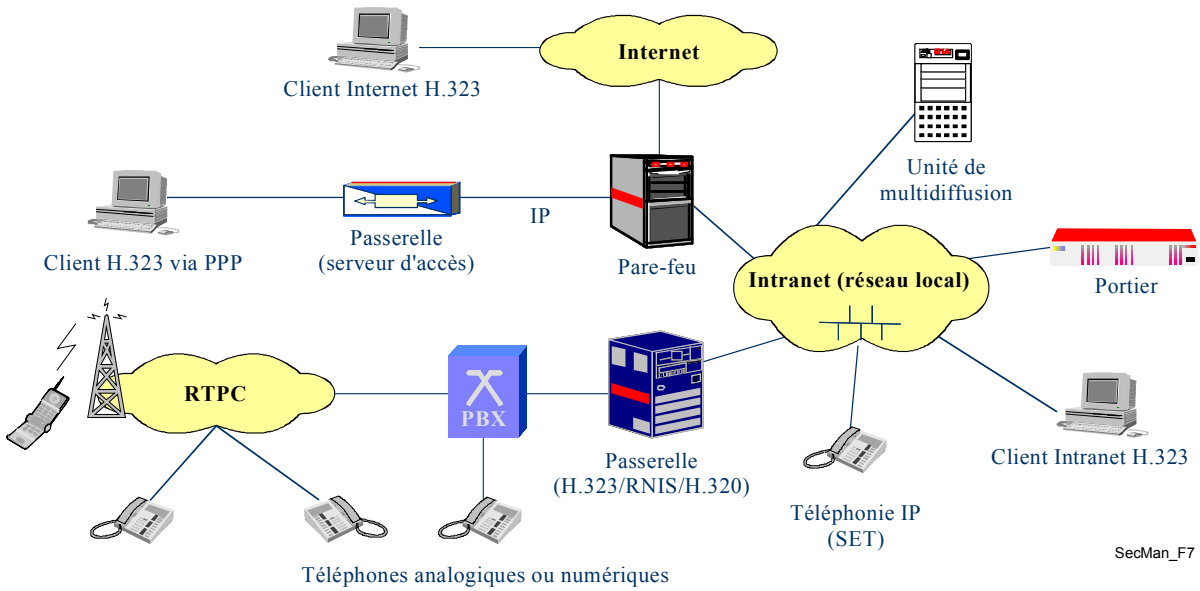
L'UIT-T a approuvé la première version de la spécification H.323 en 1996. La version 2 a été approuvée en janvier 1998 et la version actuelle (version 5) a été approuvée en juillet 2003. Cette norme au domaine d'application vaste inclut les dispositifs autonomes et les ordinateurs personnels intégrés ainsi que les conférences point à point et multipoint. Elle traite également de la commande d'appel, de la gestion multimédia et de la gestion de largeur de bande ainsi que des interfaces entre des réseaux locaux et d'autres réseaux.

La Recommandation H.323 fait partie d'une série de normes de communications permettant d'offrir des services de visioconférence dans des réseaux divers. Connue sous l'appellation H.32X, cette série comprend les Recommandations H.320 et H.324, qui portent respectivement sur les communications dans le RNIS et dans le RTPC. Le présent ouvrage donne un aperçu de la norme H.323, de ses avantages, de son architecture et de ses applications.

La Recommandation H.323 définit quatre principaux composants pour un système de communication fondé sur des réseaux: terminaux, passerelles, portiers et ponts de conférence. En outre, des éléments frontières ou homologues sont également possibles. Ces éléments apparaissent sur la Figure 7.



(a) Système H.323 et ses composants [Packetizer]



(b) Scénarios de déploiement H.323 [Euchner]

Figure 7
Système H.323: composants et scénarios de déploiement

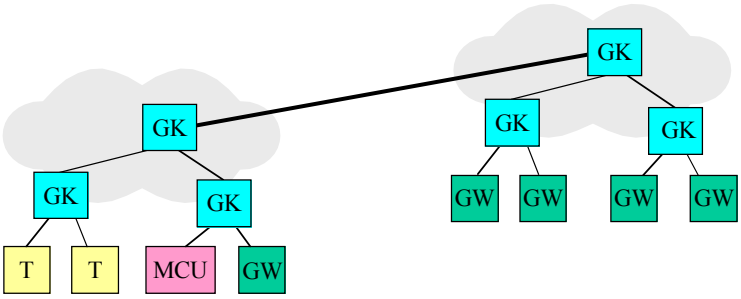
Les *terminaux (T)* sont les points d'extrémité client sur le réseau dorsal IP qui prennent en charge des communications bidirectionnelles. Les terminaux H.323 doivent prendre en charge les communications téléphoniques et peuvent prendre en charge des codecs vidéo, des protocoles de conférence de données T.120 et des capacités de pont de conférence. Ce sont par exemple des téléphones IP, des visiophones, des dispositifs à réponse vocale interactive, des systèmes de messagerie vocale, des "logiciels de téléphonie sur ordinateur" (par exemple NetMeeting™).

La *passerelle (GW, gateway)* est un élément optionnel d'une conférence H.323. Elle offre de nombreux services, le plus courant étant une fonction de traduction entre les points d'extrémité de conférence H.323 et les autres types de terminaux. Cette fonction inclut la traduction entre formats de transmission (c'est-à-dire entre H.225.0 et H.221) et entre procédures de communication (c'est-à-dire entre H.245 et H.242). En outre, la passerelle assure également la traduction entre codecs audio et vidéo et procède à l'établissement et à la libération d'appel à la fois côté réseau local et côté réseau à commutation de circuit.

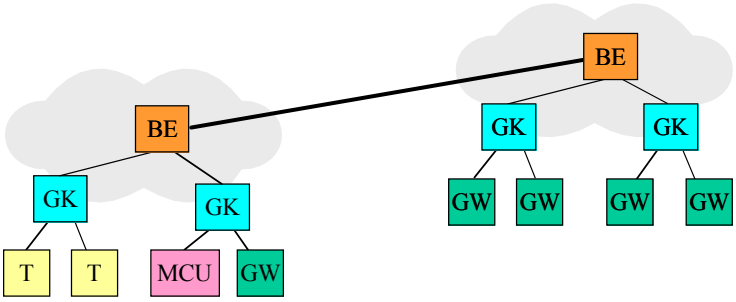
Le *portier (GK, gatekeeper)* est le composant le plus important d'un réseau de type H.323. Il est le point central pour tous les appels à l'intérieur de sa zone et offre des services de commande d'appel aux points d'extrémité enregistrés. De nombreuses façons, le portier H.323 joue le rôle de commutateur virtuel, étant donné qu'il exécute le contrôle à l'admission, la résolution d'adresse et qu'il peut autoriser le lancement direct d'appels entre points d'extrémité ou qu'il peut faire transiter la signalisation d'appel par lui afin d'exécuter des fonctions telles que suis-moi/trouves-moi, renvoi d'appel sur occupation, etc. Les portiers sont associés à des *éléments frontières* (ou homologues) *(BE, border element)*, qui sont chargés d'échanger des informations d'adressage et de participer à l'autorisation d'appel entre domaines administratifs. Cette fonctionnalité assure également l'intercommunication entre différents réseaux ou "îlots" H.323. Pour cela, une série de messages est échangée, comme illustré sur la Figure 8.

Le *pont de conférence (MCU, multipoint control unit)* prend en charge les conférences entre trois points d'extrémité ou plus. Selon la Recommandation H.323, un pont de conférence comprend un contrôleur multipoint obligatoire et zéro, un ou plusieurs processeurs multipoint. Le contrôleur multipoint gère la signalisation d'appel mais ne prend pas directement en charge les flux de médias. Cette prise en charge est assurée par les processeurs multipoint, qui mélangent, commutent et traitent les bits audio, vidéo et/ou de données. Les capacités du contrôleur multipoint et des processeurs multipoint peuvent se trouver dans un composant spécialisé ou faire partie d'autres composants H.323.

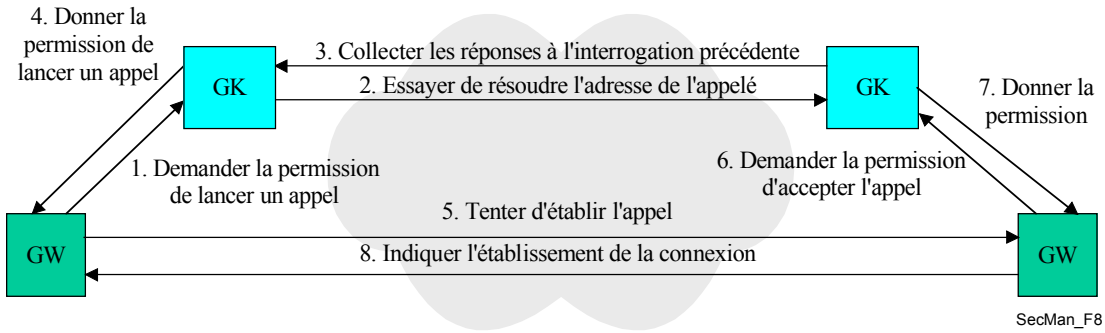
Le protocole H.323 était conçu au départ comme un protocole multimédia, mais sa principale application à ce jour est la téléphonie IP. Les réseaux H.323 actuellement en service acheminent des milliards de minutes de trafic téléphonique et vidéo par mois (dans les seuls réseaux publics); l'acheminement de la majeure partie du trafic de téléphonie IP se fait maintenant selon le protocole H.323. On estime actuellement que la téléphonie IP représente plus de 10 pour cent de toutes les minutes de communications téléphoniques internationales longue distance. Par ailleurs, le trafic vidéo H.323 augmente constamment. Ceci s'explique essentiellement par le fait que le protocole H.323 et ses mises en œuvre sont bien définis et très modulables et répondent ainsi aux besoins des fournisseurs de services et des entreprises, les produits H.323 allant de piles et de puces à des téléphones mobiles et à des matériels de visioconférence.



(a) Topologie avec le protocole RAS[1]



(b) Topologie avec le protocole de l'Annexe G/H.225.0



(c) Flux d'appel de haut niveau

Légende: BE: élément frontière; GK: portier; GW: passerelle; MCU: pont de conférence; T: terminal

Figure 8
Communications entre domaines administratifs

Les systèmes H.323 assurent les fonctionnalités suivantes:

- Capacité de conférence téléphonique, vidéo et données
- Communications entre divers types de terminaux, y compris les communications entre un ordinateur et un téléphone, entre deux télécopieurs, entre deux téléphones et les communications sur le web
- Prise en charge des télécopieurs T.38 et des modems sur IP
- De nombreux services complémentaires (renvoi d'appel, interception d'appel, etc.)

- Forte interopérabilité avec les autres systèmes H.32x, notamment H.320 (RNIS) et H.323M (systèmes hertziens mobiles 3GPP)
- Spécification de décomposition de passerelle média (via le protocole de commande de passerelle H.248)
- Prise en charge de la signalisation et de la sécurité des médias
- Mobilité d'utilisateur, de terminal et de service
- Prise en charge de la signalisation des services d'urgence

Le protocole H.323 est par exemple utilisé pour le transit en masse par les opérateurs, notamment dans les réseaux dorsaux de téléphonie IP (commutateurs de classe 4 pour le trafic téléphonique), et pour les services de carte d'appel. Dans les entreprises, le protocole H.323 est utilisé pour les autocommutateurs IP, les centrex IP, les réseaux privés virtuels téléphoniques, les systèmes téléphonie et données intégrées, les téléphones WiFi, l'implémentation de centres d'appel et les services de mobilité. A titre professionnel, les personnes l'utilisent largement pour les conférences téléphoniques (ou audio) et vidéo, pour la collaboration téléphonie/données/vidéo et pour le téléenseignement. A titre privé, elles l'emploient notamment pour l'accès audiovisuel à large bande, pour les communications entre ordinateur et téléphone et pour la diffusion d'informations et d'actualités personnalisées.

6.1.1 Problèmes de sécurité dans le domaine du multimédia et de la téléphonie IP

Comme tous les éléments d'un système H.323 peuvent être répartis géographiquement et que les réseaux IP sont ouverts, plusieurs menaces de sécurité peuvent surgir, comme l'illustre la Figure 9.

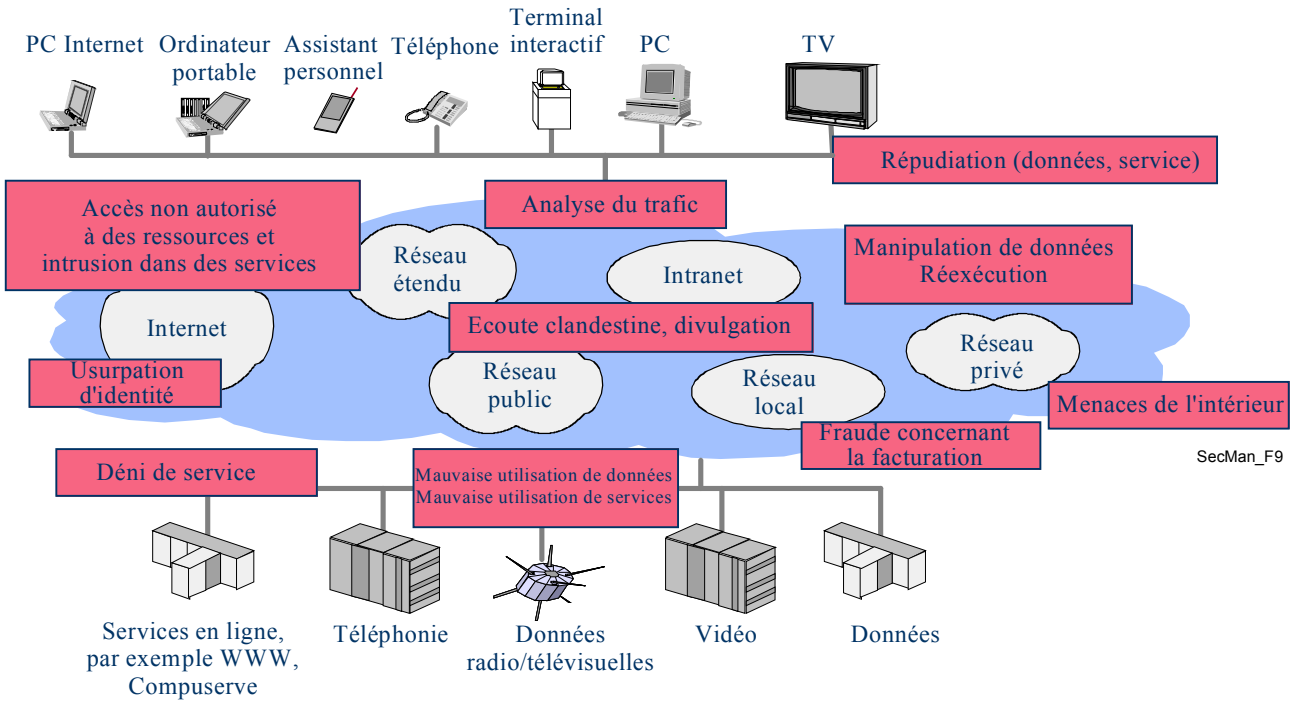


Figure 9
Menaces de sécurité dans les communications multimédias

Les principaux problèmes de sécurité qui se posent dans le domaine des communications multimédias et de la téléphonie IP en général sont les suivants [Euchner]:

- Authentification d'utilisateur et de terminal: les fournisseurs de service de téléphonie IP ont besoin de savoir qui utilise leur service pour pouvoir comptabiliser et éventuellement facturer correctement l'utilisation du service. En vue de l'authentification, l'utilisateur et/ou le terminal doit d'abord s'identifier avec une certaine identité, puis prouver que l'identité déclarée est la véritable identité. Pour cela, il est généralement fait appel à des procédures d'authentification forte par chiffrement (par exemple mot de passe protégé ou signatures numériques X.509). De même, les utilisateurs peuvent souhaiter savoir qui sont leurs correspondants téléphoniques.

- Authentification de serveur: comme les utilisateurs de téléphonie IP communiquent généralement entre eux par le biais d'une certaine infrastructure de téléphonie IP faisant intervenir des serveurs (portiers, unités de multidiffusion, passerelles), ils souhaitent savoir s'ils sont reliés au serveur correct et/ou au fournisseur de service correct. Cet aspect concerne les utilisateurs fixes comme les utilisateurs mobiles.

- Menaces de sécurité lors de l'authentification d'utilisateur/de terminal et de serveur, telles que l'usurpation d'identité, l'homme au milieu, la mystification d'adresse IP et le détournement de connexion.

- L'autorisation d'appel est le processus qui consiste à déterminer si l'utilisateur/le terminal est réellement autorisé à utiliser les ressources de service, par exemple une fonctionnalité de service (appel dans le RTPC, etc.) ou une ressource de réseau (qualité de service, largeur de bande, codec etc.). Le plus souvent, les fonctions d'authentification et d'autorisation sont rassemblées afin qu'une décision puisse être prise au niveau du contrôle d'accès. L'authentification et l'autorisation aident à contrecarrer les attaques de type usurpation d'identité, mauvaise utilisation et fraude, manipulation et déni de service.

- La protection de sécurité de la signalisation concerne la protection des protocoles de signalisation contre les manipulations et les mauvaises utilisations ainsi que la protection en termes de confidentialité et de respect de la vie privée. Les protocoles de signalisation sont généralement protégés par des moyens cryptographiques et font l'objet d'une protection d'intégrité et d'une protection contre les réexécutions. Il faut tout particulièrement veiller à ce que les facteurs de qualité critiques des communications en temps réel soient respectés et, pour cela, il faut utiliser des procédures courtes de prise de contact et des temps de transmission aller-retour courts afin d'éviter que la durée d'établissement d'une communication soit trop longue ou que la qualité téléphonique soit dégradée par suite de retards de paquets ou de gigue en raison d'un traitement de sécurité.

- La confidentialité téléphonique est assurée par le chiffrement des paquets téléphoniques, c'est-à-dire les charges utiles RTP, et par la contre-écoute des données téléphoniques surveillées. En général, les paquets de média (par exemple vidéo) d'applications multimédias sont également chiffrés. La protection renforcée des paquets de média comprend également l'authentification/la protection d'intégrité des charges utiles.

- La gestion de clés inclut non seulement toutes les tâches qui sont nécessaires pour que les parties puissent distribuer de manière sécurisée les informations relatives aux clés aux utilisateurs et aux serveurs, mais aussi les tâches liées à la mise à jour de clé en cas d'expiration ou aux clés perdues. La gestion de clés peut être exécutée en dehors de l'application de téléphonie IP (fourniture de mot de passe) ou peut être intégrée à la signalisation lorsque des profils de sécurité avec capacités de sécurité sont négociés dynamiquement et que des clés de session doivent être distribuées.

- La sécurité interdomaines se rapporte au problème découlant du fait que des systèmes appartenant à des environnements hétérogènes ont mis en œuvre des fonctionnalités de sécurité différentes en raison de besoins différents, de politiques de sécurité différentes et de capacités de sécurité différentes. Il faut donc négocier dynamiquement des profils et des capacités de sécurité tels que des algorithmes de chiffrement et leurs paramètres. Cela devient notamment important lorsque des frontières entre domaines sont franchies et que des fournisseurs et des réseaux différents interviennent. En ce qui concerne les communications interdomaines, il est important, du point de vue de la sécurité, de pouvoir traverser les pare-feu sans encombre et de pouvoir faire face aux contraintes liées aux dispositifs de traduction d'adresse de réseau (NAT, *network address translation*).

La liste n'est pas complète mais il s'agit là de l'essentiel de la sécurité H.323. En pratique, toutefois, on peut se retrouver confronté à d'autres problèmes de sécurité qui sont considérés comme ne faisant pas partie du domaine d'application du protocole H.323 (par exemple problèmes liés à la politique de sécurité, à la sécurité de gestion de réseau, à la mise en œuvre de la sécurité, à la sécurité de l'implémentation, à la sécurité opérationnelle ou au traitement des incidents de sécurité).

6.1.2 Comment la sécurité est mise en œuvre pour la téléphonie IP

La Recommandation UIT-T H.235 définit le cadre de sécurité des systèmes multimédias H.323 et spécifie notamment les mécanismes et protocoles de sécurité. Elle a été publiée pour la première fois en 1998 pour les systèmes H.323 de version 2. Depuis, elle a été étoffée: les mécanismes de sécurité offerts ont été renforcés, des algorithmes de sécurité plus sophistiqués ont été ajoutés (par exemple chiffrement AES très rapide et très sûr) et des profils de sécurité utiles et efficaces ont été élaboré pour certains scénarios d'utilisation et environnements. La version 3 de la Recommandation UIT-T H.235 – version actuellement en vigueur – offre une sécurité modulable des systèmes H.323 aussi bien pour des petits groupes que pour des entreprises ou des opérateurs à grande échelle.

En quelques mots, la Recommandation H.235 assure une protection cryptographique des protocoles de commande (RAS et signalisation d'appel H.225.0 et H.245) ainsi qu'une protection cryptographique des données de flux médias audio/vidéo. Au cours des diverses étapes de la signalisation H.323, la Recommandation H.235 offre des moyens permettant de négocier les services cryptographiques, les algorithmes de chiffrement et les capacités de sécurité souhaités et requis. Les fonctions de gestion de clés pour l'établissement de clés de session dynamiques sont entièrement intégrées aux procédures de prise de contact, ce qui permet de réduire la durée d'établissement d'appel. La gestion de clés H.235 prend en charge la configuration point à point "classique" mais aussi les configurations multipoint avec unités de multidiffusion (c'est-à-dire ponts de conférence) lorsque plusieurs terminaux multimédias communiquent dans un groupe.

La Recommandation H.235 décrit une large palette de mesures de sécurité applicables dans différents environnements cibles, par exemple les environnements intra/inter-entreprises et les environnements d'opérateurs. Suivant les hypothèses prises, par exemple en termes d'infrastructure de sécurité disponible, de capacités de terminal et de plates-formes (points d'extrémité simples ou points d'extrémité intelligents), la Recommandation H.235 offre divers profils de sécurité personnalisés et interopérables. Les profils de sécurité disponibles vont de simples profils à secret partagé avec mot de passe protégé (Annexe D/H.235 pour l'authentification et l'intégrité des messages) à des profils plus complexes avec signatures numériques et certificats PKI X.509 (Annexes E et F/H.235). Ainsi, il est possible de mettre en œuvre une protection bond par bond en utilisant les techniques les plus simples mais les moins modulables ou une protection de bout en bout en utilisant les techniques PKI modulables. L'Annexe I/H.235 assouplit la nécessité stricte d'une architecture centrée sur un serveur et avec acheminement par portier et offre des mesures de sécurité visant à sécuriser un modèle d'homologue à homologue.

La Recommandation H.235 est fondée sur des techniques de sécurité optimisées particulières (cryptographie à courbe elliptique et chiffrement AES moderne par exemple) afin de respecter les contraintes strictes de qualité. Lorsque le chiffrement téléphonique est mis en œuvre, on procède au chiffrement des charges utiles RTP dans la couche application. Cette façon de procéder est avantageuse; en effet, elle a peu d'incidence sur les points d'extrémité grâce à une interaction étroite avec le processeur de signaux numériques (DSP, *digital signal processor*) et les codecs de compression vocale et elle ne dépend pas d'une plate-forme de système d'exploitation particulière. Les outils de sécurité existants (par exemple paquetages et normes de sécurité Internet (IPSec, SSL/TLS)) qui sont disponibles et appropriés peuvent être (ré)utilisés dans le contexte de la Recommandation H.235.

La Figure 10 illustre le domaine d'application de la Recommandation H.235, qui contient des dispositions relatives à l'établissement d'appels (blocs H.225.0 et H.245) et de communications bidirectionnelles (chiffrement de charges utiles RTP contenant des signaux audio et/ou vidéo compressés). Les fonctionnalités comprennent des mécanismes pour l'authentification, l'intégrité, le respect de la vie privée et la non-répudiation. Les portiers doivent prendre en charge l'authentification en contrôlant l'admission au niveau des points d'extrémité et fournir des mécanismes de non-répudiation. La sécurité dans la couche de transport et dans les couches inférieures, fondées sur IP, sort du cadre des Recommandations H.323 et H.235, mais elle est couramment mise en œuvre au moyen des protocoles de sécurité IP (IPSec) de l'IETF et de sécurité dans la couche transport (TLS, *transport layer security*). D'une manière générale, le protocole IPSec ou TLS peut être utilisé pour assurer l'authentification et, facultativement, la confidentialité (c'est-à-dire le chiffrement) dans la couche IP quel que soit le protocole (d'application) qui est exécuté au-dessus et sans que ce protocole ne doive être mis à jour, seule la politique de sécurité à chaque extrémité doit être actualisée.

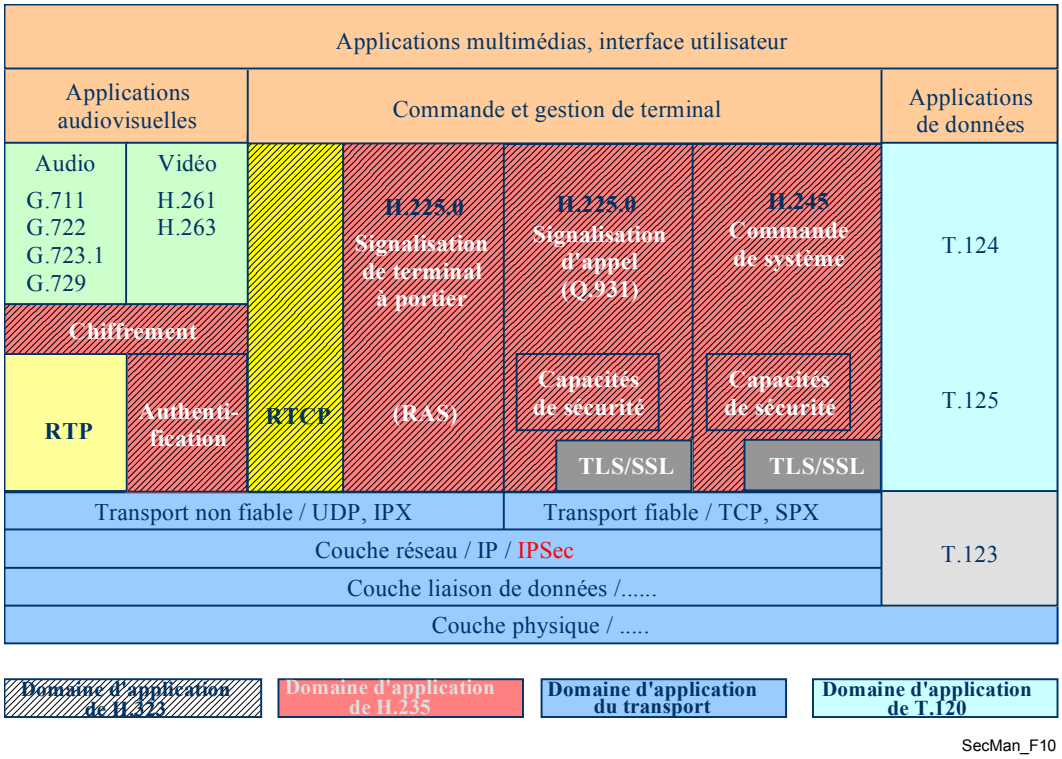


Figure 10
Sécurité des systèmes H.323 offerte par la Recommandation H.235 [Euchner]

La Recommandation H.235 s'applique essentiellement à des environnements H.323 "statiques" avec uniquement des dispositions concernant une mobilité restreinte, mais une mobilité sécurisée des utilisateurs et des terminaux dans des environnements H.323 répartis est également nécessaire au-delà de l'interconnexion interdomaines et de la mobilité restreinte dans la zone du portier. La Recommandation UIT-T H.530 répond à ces besoins de sécurité en abordant notamment les aspects de sécurité suivants:

- Authentification et autorisation d'utilisateur/de terminal mobile dans des domaines visités à l'étranger.
- Authentification du domaine visité.
- Gestion de clés sécurisée.
- Protection des données de signalisation entre un terminal mobile et un domaine visité.

En plus de la Recommandation H.235, les Recommandations H.350 et H.350.2 prévoient une gestion de clés modulable fondée sur LDAP et SSL3. La Recommandation UIT-T H.350.x définit plusieurs capacités importantes qui permettent aux entreprises et aux opérateurs de procéder à une gestion sécurisée de très nombreux utilisateurs de services de vidéo et téléphonie IP. La Recommandation H.350 permet de relier les protocoles H.323, SIP, H.320 et les services de messagerie génériques à un service d'annuaire, de manière à ce que les pratiques modernes de gestion d'identité puissent être appliquées aux communications multimédias. Par ailleurs, un endroit normalisé est réservé dans l'architecture pour stocker les pouvoirs de sécurité pour ces protocoles.

La Recommandation H.350 ne modifie les architectures de sécurité d'aucun protocole. Toutefois, elle n'offre pas d'endroit normalisé pour stocker les pouvoirs d'authentification, si besoin est. Il est à noter que les protocoles H.323 et SIP prennent tous deux en charge l'authentification par secret (Annexe D/H.235 et HTTP Digest, respectivement). Ces approches nécessitent que le serveur d'appels ait accès au mot de passe. Ainsi, si un serveur d'appels ou un annuaire H.350 est compromis, des mots de passe peuvent aussi être compromis. Ces faiblesses peuvent être dues à des faiblesses des systèmes (annuaire H.350 ou serveur d'appels) et de leur fonctionnement plutôt qu'à des faiblesses du protocole H.350 proprement dit.

Il est vivement conseillé qu'un serveur d'appels et un annuaire H.350 s'authentifient mutuellement avant de partager des informations. Il est également vivement conseillé que les communications entre annuaires H.350 et serveurs d'appels ou points d'extrémité soient établies sur des voies de communication sécurisées (par exemple SSL ou TLS).

Il est à noter que les listes de contrôle d'accès dans les serveurs LDAP dépendent de la politique appliquée et ne font pas partie de la norme. Les administrateurs de système sont invités à faire preuve de bon sens lorsqu'ils établissent un contrôle d'accès sur les attributs H.350. Par exemple, les attributs de mot de passe ne devraient être accessibles que par l'utilisateur authentifié, tandis que les attributs d'adresse peuvent être rendus publics.

6.2 Système IPCablecom

Le système IPCablecom permet aux opérateurs de télévision par câble d'offrir des services basés sur IP en temps réel (par exemple des communications téléphoniques) sur leurs réseaux qui ont été améliorés pour prendre en charge des câblomodems. L'architecture du système IPCablecom est définie dans la Recommandation UIT-T J.160. A un très haut niveau, l'architecture IPCablecom repose sur trois réseaux: le "réseau d'accès HFC J.112", le "réseau IP géré" et le RTPC. Le nœud d'accès (AN, *access node*) assure la connectivité entre le "réseau d'accès HFC J.112" et le "réseau IP géré". La passerelle de signalisation (SG, *signalling gateway*) et la passerelle média (MG, *media gateway*) assurent la connectivité entre le "réseau IP géré" et le RTPC. La Figure 11 illustre l'architecture IPCablecom de référence.

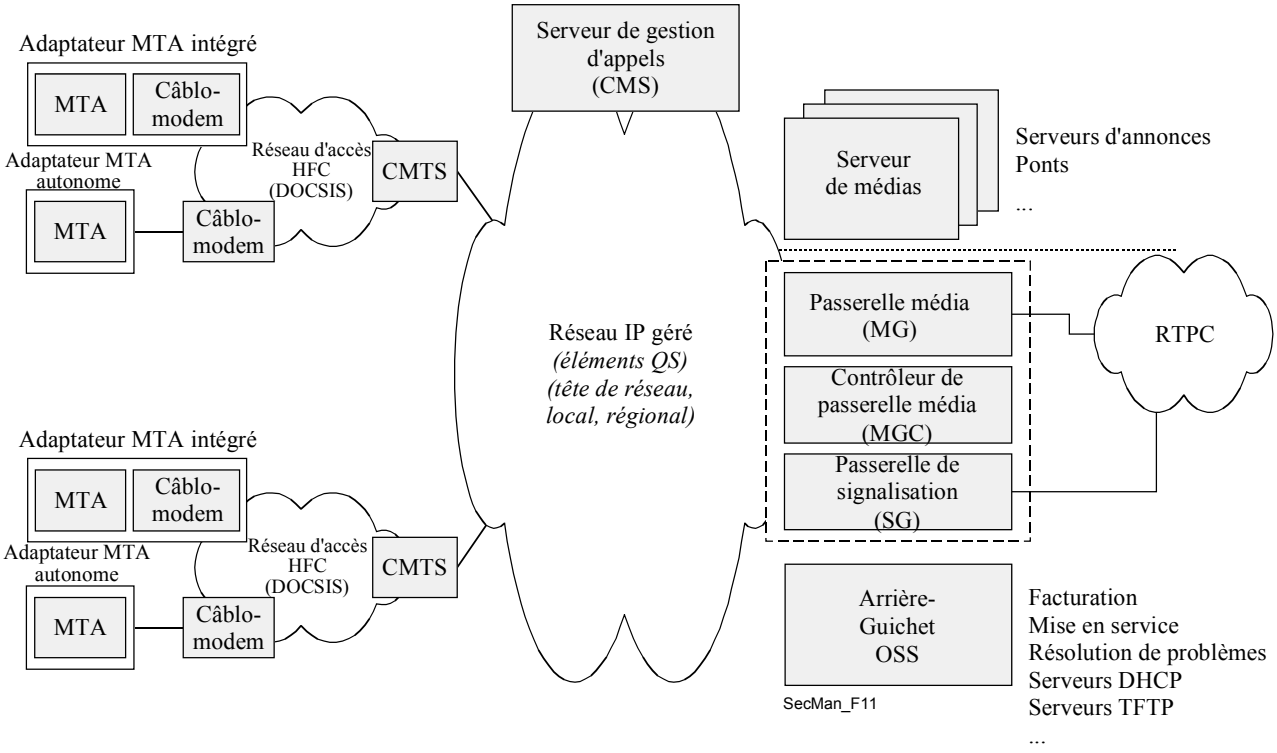


Figure 11
Architecture IPCablecom de référence [J.165]

Le réseau d'accès hybride fibre optique/câble coaxial (HFC, *hybrid fiber-coaxial cable*) J.112 assure un transport à haut débit, fiable et sécurisé entre les locaux de l'abonné et la tête de réseau câblé. Ce réseau d'accès peut offrir toutes les capacités J.112 (dont la qualité de service) et des interfaces avec la couche physique par le biais d'un système de terminaison de câblomodem (CMTS, *cable modem termination system*).

Le réseau IP géré fournit plusieurs fonctions. Il offre tout d'abord l'interconnexion entre les composants fonctionnels IPCablecom fondamentaux chargés de la signalisation, de la transmission de média, de la mise en service et de l'établissement de la qualité de service. Par ailleurs, il assure la connectivité IP longue distance entre les autres réseaux IP gérés et les réseaux HFC J.112. Le réseau IP géré est constitué des composants fonctionnels suivants: serveur de gestion d'appels, serveur d'annonces, passerelle de signalisation, passerelle média, contrôleur de passerelle média et plusieurs serveurs d'arrière du système d'appui à l'exploitation (OSS, *operational support system*).

Le *serveur de gestion d'appels* (CMS, *call management server*) offre des services liés à la commande et à la signalisation d'appel à l'adaptateur de terminal média (MTA, *media terminal adapter*), au nœud d'accès et aux passerelles RTPC du réseau IPCablecom. Le serveur CMS est un élément de réseau sécurisé qui se trouve dans la partie IP gérée du réseau IPCablecom. Les *serveurs d'annonces* sont des composants de réseau logiques qui gèrent et passent des tonalités et messages d'information en réponse à des événements qui se produisent dans le réseau. La fonction de *passerelle de signalisation* envoie et reçoit la signalisation de réseau à commutation de circuit à la frontière du réseau IPCablecom. Pour le système IPCablecom, cette fonction ne prend en charge que la signalisation autre que service par service sous la forme de messages SS7 (la signalisation service par service sous la forme de tonalités

multifréquences est directement prise en charge par la fonction de passerelle média). Le *contrôleur de passerelle média* (MGC, *media gateway controller*) sert d'intermédiaire entre le réseau IPCablecom et le RTPC concernant les informations de signalisation d'appel. Il maintient et contrôle l'état d'appel global pour les appels nécessitant une interconnexion avec le RTPC. La *passerelle média* (MG, *media gateway*) assure la connectivité des supports entre le RTPC et le réseau IPCablecom. Chaque support est représenté sous la forme d'un point d'extrémité et le contrôleur MGC charge la passerelle média d'établir et de contrôler les connexions de média vers les autres points d'extrémité du réseau IPCablecom. Le contrôleur MGC charge également la passerelle média de détecter et de générer des événements et des signaux relatifs à l'état d'appel. Le *système arrière-guichet OSS* contient des composants de gestion commerciale, de gestion de service et de gestion de réseau servant d'appui aux processus d'exploitation centraux. Les principales fonctions du système OSS sont les suivantes: gestion des défauts, gestion de la qualité de fonctionnement, gestion de la sécurité, gestion de la comptabilité et gestion de la configuration. L'architecture IPCablecom définit un ensemble limité de composants fonctionnels et d'interfaces OSS pour prendre en charge la configuration des dispositifs MTA et la messagerie d'événements en vue de l'acheminement des informations de facturation.

6.2.1 Problèmes de sécurité dans le système IPCablecom

Chacune des interfaces de protocole IPCablecom est exposée à des menaces qui peuvent entraîner des risques de sécurité à la fois pour l'abonné et pour le fournisseur de services. Par exemple, le trajet du flux de média peut emprunter un grand nombre de connexions d'opérateurs de réseaux dorsaux qui peuvent être inconnus. Le flux de média est alors vulnérable aux écoutes malveillantes entraînant une perte de la confidentialité des communications.

6.2.2 Mécanismes de sécurité dans le système IPCablecom

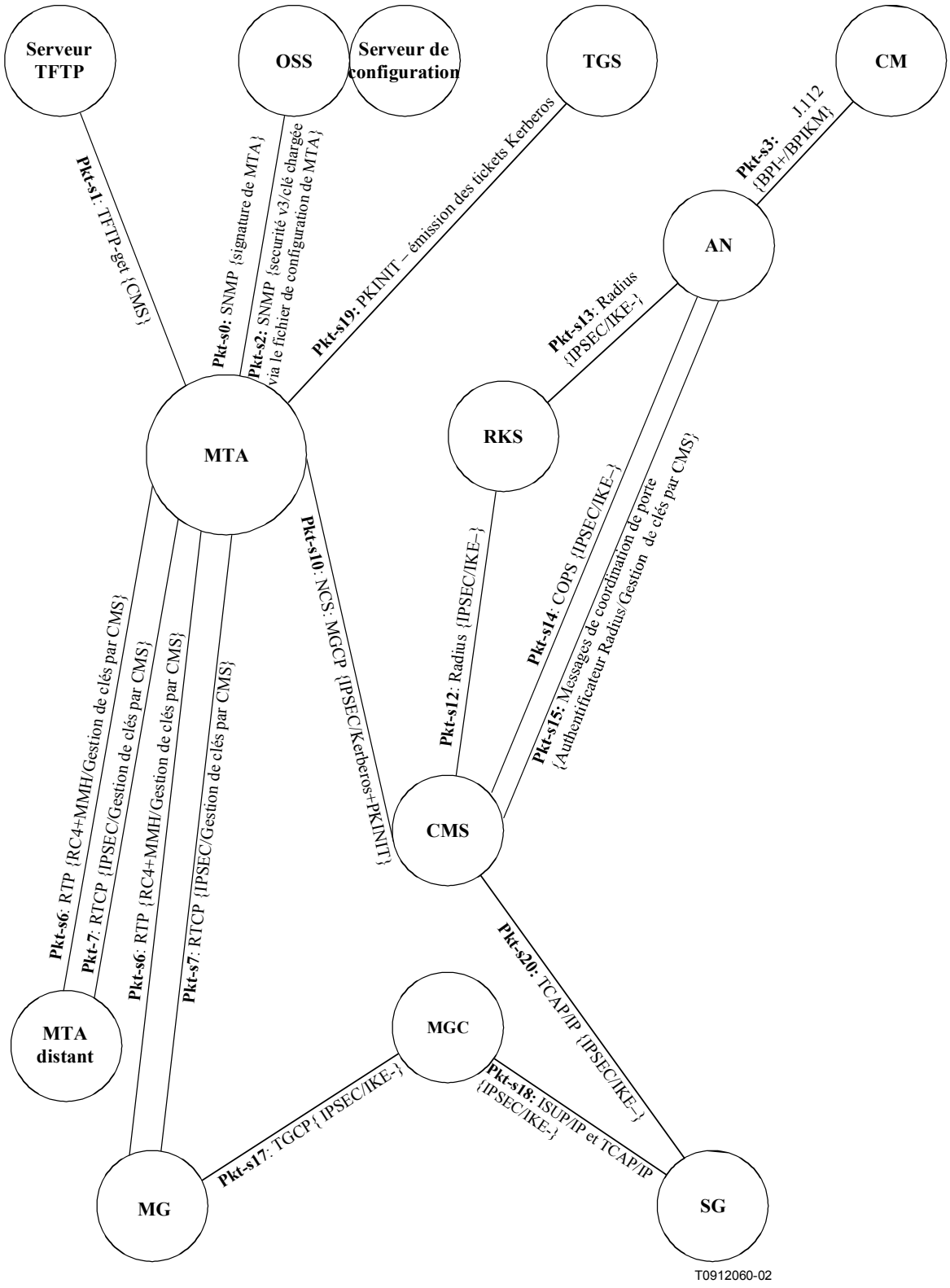
Dans le système IPCablecom, la sécurité est mise en œuvre dans les éléments les plus bas de la pile et utilise donc essentiellement des mécanismes définis par l'IETF. L'architecture IPCablecom fait face aux menaces en spécifiant, pour chaque interface de protocole définie, les mécanismes de sécurité sous-jacents (tels que IPsec) qui offrent à l'interface les services de sécurité dont elle a besoin. Dans le contexte de l'architecture X.805, les services de sécurité définis pour IPCablecom concernent les neuf cellules résultant des trois plans et des trois couches de la Figure 1. Par exemple, les services de sécurité des protocoles de signalisation pour le plan de commande sont assurés par le protocole IPSec. La sécurité de l'infrastructure de gestion est obtenue grâce au protocole SNMP v3.

Les services de sécurité disponibles par l'intermédiaire de la couche des services essentiels de l'architecture IPCablecom sont les suivants: authentification, contrôle d'accès, intégrité, confidentialité et non-répudiation. Une interface de protocole IPCablecom peut employer zéro, un ou plusieurs de ces services pour répondre à ses besoins de sécurité particuliers.

La sécurité IPCablecom répond aux exigences de sécurité de chaque interface de protocole constituante en:

- identifiant le modèle de menaces propre à chaque interface de protocole constituante;
- identifiant les services de sécurité (authentification, autorisation, confidentialité, intégrité et non-répudiation) requis pour faire face aux menaces identifiées;
- spécifiant le mécanisme de sécurité particulier qui assure les services de sécurité requis.

Les mécanismes de sécurité comprennent à la fois le protocole de sécurité (par exemple IPsec, sécurité de couche RTP et sécurité SNMPv3) et le protocole de gestion de clés support (par exemple IKE, PKINIT/Kerberos). Par ailleurs, les services essentiels de sécurité IPCablecom incluent un mécanisme assurant le chiffrement de bout en bout des flux de média RTP, ce qui réduit fortement la menace de perte de confidentialité. La Figure 12 récapitule toutes les interfaces de sécurité IPCablecom. Si le protocole de gestion de clés n'est pas indiqué, c'est qu'il n'est pas nécessaire pour l'interface considérée. Les interfaces IPCablecom qui n'ont pas besoin de sécurité ne sont pas représentées sur la Figure 12.



IKE – IKE avec clés préalablement prépartagées
IKE+ IKE nécessitant des certificats de clé publique
Gestion de clés par CMS Clés générées aléatoirement et distribuées par le serveur CMS

Figure 12
Interfaces de sécurité IPCablecom (étiquetées sous la forme <étiquette>: <protocole> { <protocole de sécurité> / <protocole de gestion de clés > })

L'architecture de sécurité IPCablecom subdivise la mise en service de dispositif en trois activités distinctes: inscription de l'abonné, mise en service du dispositif et autorisation du dispositif. Le processus d'*inscription de l'abonné* établit un compte permanent de facturation de l'abonné qui identifie de manière univoque l'adaptateur MTA auprès du serveur CMS grâce au numéro de série ou à l'adresse MAC de l'adaptateur MTA. Le compte de facturation sert également à identifier les services auxquels l'abonné a souscrit pour l'adaptateur MTA. L'inscription de l'abonné peut se faire dans la bande ou hors bande. La spécification proprement dite du processus d'inscription de l'abonné sort du cadre de l'architecture IPCablecom et peut varier d'un fournisseur de service à l'autre. Pour la *mise en service du dispositif*, l'adaptateur MTA vérifie l'authenticité du fichier de configuration qu'il télécharge en commençant par établir la sécurité SNMPv3 (en utilisant une authentification de type Kerberos et une gestion de clés) entre lui-même et le serveur de mise en service. Le serveur de mise en service fournit ensuite à l'adaptateur MTA l'emplacement du fichier de configuration et une valeur de hachage du fichier de configuration. L'adaptateur MTA extrait le fichier de configuration, applique un hachage au fichier de configuration et compare le résultat avec la valeur de hachage que le serveur de mise en service lui a fournie. Le fichier de configuration est authentifié si les valeurs de hachage concordent. Le fichier de configuration peut facultativement être chiffré à des fins de confidentialité (la confidentialité SNMPv3 doit aussi être prise en charge afin d'assurer une transmission sécurisée de la clé de chiffrement du fichier de configuration à l'adaptateur MTA). L'*autorisation du dispositif* est le processus selon lequel l'adaptateur MTA mis en service s'authentifie auprès du serveur de gestion d'appels et établit une association de sécurité avec ce serveur avant de devenir entièrement opérationnel. L'autorisation de dispositif permet de protéger la signalisation d'appel subséquente dans le cadre de l'association de sécurité établie.

Il est possible de protéger à la fois le trafic de signalisation et les flux de média. L'ensemble du trafic de signalisation, qui comprend la signalisation de qualité de service, la signalisation d'appel et la signalisation avec l'interface de passerelle RTPC, sera sécurisé au moyen du protocole IPsec. Les associations de sécurité IPsec seront gérées grâce à l'utilisation de deux protocoles de gestion de clés: Kerberos/PKINIT et IKE. Le protocole Kerberos/PKINIT sera utilisé pour échanger des clés entre des clients d'adaptateur MTA et leur serveur CMS; le protocole IKE sera utilisé pour gérer toutes les autres associations de sécurité IPsec de signalisation. En ce qui concerne les flux de média, chaque paquet RTP de média est chiffré aux fins de confidentialité et authentifié afin de vérifier l'intégrité et l'origine du paquet. Les adaptateurs MTA ont la capacité de négocier un algorithme de chiffrement particulier, bien que le seul algorithme de chiffrement requis soit AES. Chaque paquet RTP peut facultativement inclure un code d'authentification de message (MAC, *message authentication code*). L'algorithme de calcul du code MAC peut aussi être négocié, bien que le seul à être actuellement spécifié soit MMH. Le calcul du code MAC englobe l'en-tête non chiffré et la charge utile chiffrée du paquet.

Les clés de chiffrement et le calcul du code MAC sont déterminés à partir du secret de bout en bout et des données de remplissage facultatives, qui sont échangés entre les adaptateurs MTA d'émission et de réception dans le cadre de la signalisation d'appel. Les échanges de clés pour la sécurité des flux de média sont donc eux-mêmes sécurisés par la protection de la signalisation d'appel.

La sécurité est également assurée pour le système OSS et le système de facturation. Les agents SNMP présents dans les dispositifs IPCablecom implémentent le protocole SNMPv3. Le modèle de sécurité d'utilisateur SNMPv3 [RFC 2274] offre des services d'authentification et de confidentialité concernant le trafic SNMP. Le contrôle d'accès de type vue SNMPv3 [RFC 2275] peut être utilisé pour le contrôle d'accès à des objets MIB.

Le protocole de gestion de clés IKE sert à établir des clés de chiffrement et d'authentification entre le serveur d'archivage (RKS, *record keeping server*) et chaque élément de réseau IPCablecom qui génère des messages d'événement. Lorsque des associations de sécurité IPsec de réseau sont établies, ces clés doivent être créées entre chaque serveur RKS (primaire, secondaire, etc.) et chaque serveur CMS et nœud d'accès. Un échange de clés entre le contrôleur MGC et le serveur RKS peut être prévu; il appartient aux fabricants de l'implémenter ou non dans la phase 1 de l'architecture IPCablecom,. Les messages d'événement sont envoyés par le serveur CMS et par le nœud d'accès au serveur RKS au moyen du protocole de transport RADIUS, qui est lui-même sécurisé par IPsec.

6.3 Transmission de télécopie sécurisée

La télécopie est une application très courante. La transmission de télécopie était définie au départ sur le RTPC (UIT-T T.4), puis également sur le RNIS (UIT-T T.6) et, plus récemment, aussi sur les réseaux IP (y compris l'Internet) pas en temps réel – relais par messagerie électronique – (UIT-T T.37) ou en temps réel – en utilisant le protocole RTP – (UIT-T T.38). Deux problèmes de sécurité généralement rencontrés par la transmission de télécopie – que le réseau soit un RTPC, un RNIS ou un réseau IP – concernent l'authentification (et parfois la non-répudiation) d'une connexion et la confidentialité des données transmises. Ces problèmes sont d'autant plus importants pour les protocoles T.37 et T.38 que le réseau IP est, par nature, réparti.

La Recommandation UIT-T T.36 définit deux solutions techniques indépendantes qui peuvent être utilisées dans le contexte de la transmission de télécopie sécurisée pour le chiffrement des documents échangés. Les deux solutions techniques s'appuient sur les algorithmes HKM/HFX40 (Annexe A/T.36) et l'algorithme RSA (Annexe B/T.36). Même si les deux limitent les clés de session à 40 bits (en raison de réglementations nationales au moment de l'approbation de la Recommandation, 1997), un mécanisme est spécifié afin de générer une clé de session redondante (à partir d'une clé de session de 40 bits) pour les algorithmes qui nécessitent des clés plus longues. L'Annexe C/T.36 décrit l'utilisation du système HKM offrant des capacités de gestion de clés sécurisée pour les télécopieurs grâce à un enregistrement unidirectionnel entre les entités X et Y ou à la transmission sécurisée d'une clé secrète entre les entités X et Y. L'Annexe D/T.36 définit les procédures d'utilisation du système de chiffrement HFX40 qui permet d'assurer la confidentialité des messages de télécopie. Enfin, l'Annexe E/T.36 décrit l'utilisation de l'algorithme de hachage HFX40-I, les calculs nécessaires et les informations à échanger entre les télécopieurs afin d'assurer l'intégrité d'un message de télécopie transmis, cet algorithme étant choisi ou préprogrammé remplacement du chiffrement du message.

De plus, la Recommandation T.36 définit les services de sécurité suivants:

- Authentification mutuelle (obligatoire).
- Service de sécurité (facultatif) incluant l'authentification mutuelle, l'intégrité de message et la confirmation de réception de message.
- Service de sécurité (facultatif) incluant l'authentification mutuelle, la confidentialité de message (chiffrement) et l'établissement de clé de session.
- Service de sécurité (facultatif) incluant l'authentification mutuelle, l'intégrité de message, la confirmation de réception de message, la confidentialité de message (chiffrement) et l'établissement de clé de session.

Quatre profils de service sont définis sur la base des services de sécurité énumérés ci-dessus, comme indiqué dans le Tableau 2 ci-dessous.

Tableau 2
Profils de sécurité de l'Annexe H/T.30

Services de sécurité	Profils de service			
	1	2	3	4
Authentification mutuelle	X	X	X	X
• Intégrité de message • Confirmation de réception de message		X		X
• Confidentialité de message (chiffrement) • Etablissement de clé de session			X	X

6.3.1 Sécurité de la transmission de télécopie fondée sur les systèmes HKM et HFX

La combinaison des systèmes HKM (*Hawthorne Key Management*) et HFX (*Hawthorne Facsimile Cipher*) offre les capacités de sécurité suivantes concernant les communications de document entre entités (terminaux ou opérateurs de terminal):

- authentification mutuelle d'entités;
- établissement de clé de session secrète;
- confidentialité de document;
- confirmation de réception;
- confirmation on réfutation d'intégrité de document.

La gestion de clés est assurée par le système HKM défini dans l'Annexe B/T.36. Deux procédures sont définies, la première étant l'enregistrement et la seconde la transmission sécurisée d'une clé secrète. L'enregistrement établit des secrets mutuels et permet de sécuriser toutes les transmissions suivantes. Dans les transmissions suivantes, le système HKM assure l'authentification mutuelle, établit une clé de session secrète pour la confidentialité et l'intégrité de document et prend en charge la confirmation de réception et la confirmation ou la réfutation d'intégrité de document.

La confidentialité de document est assurée par le système de chiffrement défini dans l'Annexe D/T.36. Ce système utilise une clé de 12 chiffres décimaux, ce qui correspond approximativement à une clé de session de 40 bits.

L'intégrité de document est assurée par le système défini dans l'Annexe E/T.36 et la Recommandation T.36 définit l'algorithme de hachage, y compris les calculs et l'échange d'informations associés.

Dans le mode enregistrement, les deux terminaux échangent des informations qui permettent aux entités de s'identifier mutuellement de manière univoque. Dans ce mode, les utilisateurs conviennent d'une clé secrète à usage unique. Chaque entité stocke un nombre de 16 chiffres qui est associé de manière univoque à l'entité avec laquelle elle a procédé à l'enregistrement.

Lorsqu'un terminal émetteur doit procéder à l'envoi sécurisé d'un document, il envoie à l'entité réceptrice le nombre secret de 16 chiffres associé à l'entité réceptrice ainsi qu'un nombre aléatoire et une clé de session chiffrée en tant qu'épreuve. Le terminal récepteur répond en envoyant la clé de 16 chiffres associée à l'entité émettrice ainsi qu'un nombre aléatoire et une version rechiffrée de l'épreuve provenant de l'entité émettrice. En même temps, il envoie à l'entité émettrice un nombre aléatoire et une clé de session chiffrée en tant qu'épreuve. Le terminal émetteur répond par un nombre aléatoire et une version rechiffrée de l'épreuve provenant de l'entité réceptrice. Cette procédure permet aux deux entités de s'authentifier mutuellement. En même temps, le terminal émetteur envoie un nombre aléatoire et la clé de session chiffrée à utiliser pour le chiffrement et le hachage.

Après la transmission du document, le terminal émetteur envoie à l'entité réceptrice un nombre aléatoire et une clé de session chiffrée en tant qu'épreuve. En même temps, il envoie un nombre aléatoire et une valeur de hachage chiffrée permettant à l'entité réceptrice de vérifier l'intégrité du document reçu. Le terminal récepteur envoie un nombre aléatoire et la version rechiffrée de l'épreuve provenant de l'entité émettrice. En même temps, il envoie un nombre aléatoire et un message d'intégrité chiffré pour confirmer ou réfuter l'intégrité du document reçu. L'algorithme de hachage utilisé pour l'intégrité du document est appliqué à l'ensemble du document.

Un mode de remplacement est prévu, qui ne fait pas intervenir d'échange de signaux de sécurité entre les deux terminaux. Les utilisateurs s'entendent sur une clé de session secrète à usage unique qui doit être saisie manuellement. Le terminal émetteur utilise cette clé pour chiffrer le document et le terminal récepteur l'utilise pour déchiffrer le document.

6.3.2 Sécurité de la transmission de télécopie fondée sur l'algorithme RSA

L'Annexe H/T.30 spécifie les mécanismes permettant d'offrir des éléments de sécurité sur la base du mécanisme cryptographique RSA (*Rivest, Shamir & Adleman*). Pour avoir des détails sur l'algorithme RSA, on se reportera au document [ApplCryp, pages 466 à 474]. N'importe lequel des systèmes de codage définis dans les Recommandations T.4 et T.30 (Huffman modifié, MR, MMR, mode caractère tel que défini dans l'Annexe D/T.4, BFT, autre mode de transfert de fichier défini dans l'Annexe C/T.4) est applicable dans le cas d'un document transmis sous couvert d'éléments de sécurité.

L'algorithme de base utilisé pour la signature numérique (services des types authentification et intégrité) est l'algorithme RSA utilisant une paire "clé publique"/"clé secrète".

Lorsque le service facultatif de confidentialité est offert, le jeton contenant la clé de session "Ks" utilisée pour le chiffrement du document, est chiffré, lui aussi, au moyen de l'algorithme RSA. La paire de clés utilisée à cette fin, appelée "clé publique de chiffrement"/"clé secrète de chiffrement", n'est pas la même que celle qui est utilisée pour les services des types authentification et intégrité. Ainsi, les deux types d'utilisation sont découplés.

L'implémentation de l'algorithme RSA utilisé dans l'Annexe H est décrite dans la norme ISO/CEI 9796 (Schémas de signature numérique rétablissant le message).

Concernant le chiffrement du jeton contenant la clé de session, les règles de redondance appliquées lors de l'utilisation de l'algorithme RSA sont les mêmes que celles qui sont spécifiées dans la norme ISO/CEI 9796. Il est à noter que certaines administrations pourront exiger l'implémentation de l'algorithme DSA (*Digital Signature Algorithm*) [ApplCryp, pp-483-502] en plus de l'algorithme RSA.

Par défaut, les *autorités de certification* ne sont pas utilisées dans le schéma de l'Annexe H/T.30, elles peuvent toutefois être facultativement utilisées pour certifier la validité de la clé publique de l'émetteur du message de télécopie. En pareil cas, la clé publique peut être certifiée conformément aux spécifications figurant dans la Recommandation X.509. La méthode à utiliser pour transmettre le certificat de la clé publique de l'émetteur est décrite à l'Annexe H, mais le format précis du certificat sera étudié ultérieurement et la transmission effective du certificat est négociée dans le protocole.

Un *mode enregistrement* est prévu en tant que fonctionnalité obligatoire. Il permet à l'émetteur et au récepteur d'enregistrer et de stocker les clés publiques de l'autre partie de manière fiable avant toute communication de télécopie sécurisée entre les deux parties. Le mode enregistrement permet d'éviter à l'utilisateur de devoir saisir manuellement les clés publiques de ses correspondants, qui sont relativement longues (64 octets au moins).

Comme le mode enregistrement permet d'échanger les clés publiques et de les stocker dans les terminaux, il n'est pas nécessaire de les transmettre pendant les communications de télécopie.

Comme décrit dans cette annexe, certaines signatures sont appliquées au résultat d'une "fonction de hachage".

Les fonctions de hachage qui peuvent être utilisées sont l'algorithme SHA-1 (*Secure Hash Algorithm*), élaboré par le National Institute of Standards and Technology (NIST) aux Etats-Unis d'Amérique, ou le MD-5 (RFC 1321). Dans le cas de SHA-1, la longueur du résultat du processus de hachage est de 160 bits et dans le cas de MD-5, la longueur du résultat du processus de hachage est de 128 bits. Un terminal conforme à l'Annexe H/T.30 peut implémenter soit le SHA-1, soit le MD-5 soit les deux. L'utilisation de l'un ou l'autre algorithme est négociée dans le protocole (voir plus loin).

Le chiffrement des données aux fins de confidentialité est facultatif. Cinq mécanismes de chiffrement facultatifs sont enregistrés dans le cadre de l'Annexe H/T.30: FEAL-32, SAFER K-64, RC5, IDEA et HFX40 (comme décrit dans la Recommandation T.36). Dans certains pays, leur utilisation peut être assujettie à la réglementation nationale.

Il est aussi permis d'employer d'autres algorithmes facultatifs, choisis conformément à la norme ISO/CEI 9979 (Procédures d'enregistrement des algorithmes cryptographiques).

La capacité du terminal à manipuler l'un de ces algorithmes et l'utilisation effective d'un algorithme particulier pendant une communication donnée sont négociées dans le protocole. Une clé de session est utilisée pour le chiffrement. La longueur de base d'une clé de session est de 40 bits. Pour les algorithmes qui utilisent une clé de session de 40 bits (par exemple HFX40), la clé de session "Ks" est la clé effectivement utilisée dans l'algorithme de chiffrement et pour les algorithmes qui nécessitent des clés plus longues que 40 bits (par exemple les algorithmes FEAL-32, IDEA et SAFER K-64 qui nécessitent respectivement des clés de 64 bits, 128 bits et 64 bits), un mécanisme de redondance est exécuté afin d'obtenir la longueur nécessaire. La clé résultante est appelée "clé de session redondante". La "clé de session redondante" est la clé qui est effectivement utilisée dans l'algorithme de chiffrement.

6.4 Applications de gestion de réseau

Comme indiqué dans le paragraphe sur la nécessité d'un cadre de sécurité, il est impératif de sécuriser le trafic de gestion utilisé pour surveiller et contrôler le réseau de télécommunication. Le trafic de gestion est généralement classé dans différentes catégories en fonction des informations requises pour exécuter les fonctions de gestion des défauts, de la configuration, de la qualité de fonctionnement, de la comptabilité et de la sécurité. La gestion de la sécurité concerne à la fois l'établissement d'un réseau de gestion sécurisé et la gestion de la sécurité des informations liées aux trois plans de sécurité et aux trois couches de sécurité de l'architecture de sécurité. Le deuxième point est décrit dans le présent paragraphe.

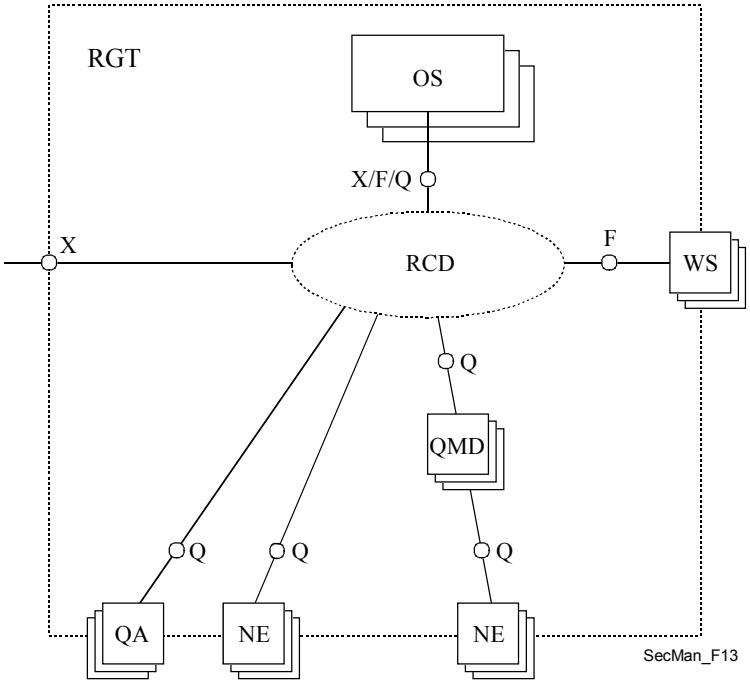
Traditionnellement, dans le réseau de télécommunication, le trafic de gestion est souvent transmis dans un réseau distinct qui achemine uniquement le trafic de gestion de réseau et non le trafic des utilisateurs. Ce réseau, souvent appelé réseau de gestion des télécommunications (RGT), est décrit dans la Recommandation UIT-T M.3010. Le RGT est séparé et isolé de l'infrastructure du réseau public de sorte que les perturbations dues à des menaces de sécurité dans le plan d'utilisateur final du réseau public ne s'étendent pas au RGT. Compte tenu de cette séparation, il est relativement facile de sécuriser le trafic du réseau de gestion car l'accès au plan de gestion est restreint aux administrateurs de réseau autorisés et le trafic est restreint aux activités de gestion valables. Avec la mise en place des réseaux de la prochaine génération, le trafic des applications d'utilisateur final risque parfois d'être combiné au trafic de gestion. Cette approche, fondée sur une seule infrastructure de réseau intégrée, permet de minimaliser les coûts mais pose bon nombre de nouveaux problèmes de sécurité. Les menaces dans le plan d'utilisateur final constituent alors des menaces pour les plans de gestion et de commande. Le plan de gestion devient alors accessible à une multitude d'utilisateurs finaux et de nombreux types d'activités malveillantes deviennent possibles.

Pour pouvoir offrir une solution complète de bout en bout, toutes les mesures de sécurité (par exemple contrôle d'accès, authentification) doivent être appliquées à chaque type d'activité de réseau (c'est-à-dire activité du plan de gestion, activité du plan de commande et activité du plan d'utilisateur final) concernant l'infrastructure du réseau, les services de réseau et les applications de réseau. Il existe un certain nombre de Recommandations de l'UIT-T qui portent tout particulièrement sur l'aspect de sécurité du plan de gestion en ce qui concerne les éléments de réseau (NE, *network element*) et les systèmes de gestion (MS, *management system*) qui font partie de l'infrastructure du réseau.

Comme décrit ci-dessus, de nombreuses normes visent à sécuriser les informations de gestion nécessaires au maintien de l'infrastructure des télécommunications, mais un autre domaine qui relève de la gestion concerne les environnements dans lesquels différents fournisseurs de services doivent interagir pour offrir des services de bout en bout, par exemple une ligne louée entre des abonnés se trouvant de part et d'autre d'une frontière géographique ou pour des organismes de réglementation ou des organismes publics en vue d'assurer le retour à la normale après une catastrophe.

6.4.1 Architecture de gestion de réseau

L'architecture permettant de définir la gestion d'un réseau de télécommunication est définie dans la Recommandation M.3010 et l'architecture physique est représentée sur la Figure 13. Le réseau de gestion définit des interfaces qui déterminent les échanges requis pour assurer les fonctions OAM&P à différents niveaux.



interfaces
RCD réseau de communication de données
NE élément de réseau
OS système d'exploitation
WS poste de travail

Figure 13
Exemple d'architecture physique (M.3010)

Les exigences de sécurité varient d'une interface à l'autre. L'interface Q se trouve dans un seul domaine administratif tandis que l'interface X se trouve entre différents domaines administratifs qui peuvent appartenir à différents fournisseurs. Des services de sécurité sont nécessaires pour les deux interfaces, mais les contre-mesures requises pour l'interface X sont plus robustes. La Recommandation UIT-T M.3016 donne un aperçu des menaces et vulnérabilités de sécurité et des mesures de sécurité applicables à ces interfaces, la Recommandation UIT-T M.3320 détaillant les aspects propres à l'interface X. Les aspects de protocole applicables aux différentes couches de communication sont spécifiés dans les Recommandations UIT-T Q.811 et Q.812.

Lorsqu'on examine la sécurité dans le contexte de la gestion, deux facettes sont à prendre en considération. La première concerne le plan de gestion pour une activité de bout en bout (par exemple services de téléphonie IP). L'activité de gestion consistant à administrer les utilisateurs doit être réalisée de manière sécurisée. On parle de *sécurité des informations de gestion* échangées sur le réseau pour le déploiement d'une application de bout en bout. La deuxième facette est la gestion des informations de sécurité. Quelle que soit l'application (par exemple téléphonie IP ou activité de signalisation de dérangement entre deux fournisseurs de service), des mesures de sécurité telles que l'utilisation de clés de chiffrement doivent aussi être gérées. On parle souvent de *gestion des informations de sécurité*. L'infrastructure PKI définie au paragraphe précédent est un exemple de cette facette. La Recommandation UIT-T M.3400 définit un certain nombre de fonctions liées à ces deux facettes.

Sur la base du cadre défini dans la Recommandation X.805, plusieurs Recommandations portant sur des fonctions de gestion sont disponibles pour les trois cellules du plan de gestion. Les paragraphes qui suivent illustrent certaines de ces Recommandations et montrent comment les besoins de sécurité sont pris en considération. En plus des Recommandations relatives aux trois cellules du plan de gestion, il en existe d'autres qui définissent des services génériques ou communs, par exemple l'envoi d'alarme en cas de violation de sécurité physique, des fonctions d'audit et des modèles d'information définissant des niveaux de protection pour différentes cibles (c'est-à-dire les entités de gestion).

6.4.2 Intersection du plan de gestion et de la couche infrastructure

Cette cellule concerne la sécurisation de l'activité de gestion des éléments d'infrastructure du réseau, à savoir les éléments de commutation et de transmission et les liaisons entre ces éléments ainsi que les systèmes d'extrémité tels que les serveurs. Les activités telles que la configuration d'un élément de réseau doivent par exemple être réalisées par un utilisateur autorisé. Une connectivité de bout en bout peut être envisagée en termes de réseaux d'accès et de réseaux centraux. Différentes technologies peuvent être employées dans ces réseaux. Des Recommandations ont été élaborées pour les deux types de réseau (réseau d'accès et réseau central). On prend ici l'exemple du réseau optique passif à large bande (BPON, *broadband passive optical network*) utilisé comme réseau d'accès. L'administration des privilèges des utilisateurs pour un tel réseau d'accès est définie au moyen de la méthodologie de modélisation unifiée dans la Recommandation Q.834.3 et l'échange de gestion utilisant l'architecture de courtier commun de requêtes d'objets (CORBA, *common object request broker architecture*) est spécifié dans la Recommandation Q.834.4. L'interface décrite dans ces Recommandations est l'interface Q illustrée sur la Figure 13. Elle est appliquée entre le système de gestion des éléments et le système de gestion du réseau. Le système de gestion des éléments sert à gérer les différents éléments de réseau et a donc connaissance des détails internes des architectures matérielle et logicielle des éléments d'un ou de plusieurs fournisseurs et le système de gestion du réseau réalise les activités au niveau du réseau de bout en bout et couvre les systèmes de gestion de plusieurs fournisseurs. La Figure 14 montre les divers objets utilisés pour créer, supprimer, attribuer et utiliser des informations de contrôle d'accès pour les utilisateurs du système de gestion des éléments. La liste de permissions des utilisateurs contient, pour chaque utilisateur autorisé, la liste des activités de gestion qui sont permises. Le gestionnaire de contrôle d'accès vérifie l'identité et le mot de passe de l'utilisateur de l'activité de gestion et autorise l'accès à la fonctionnalité figurant dans la liste de permissions.

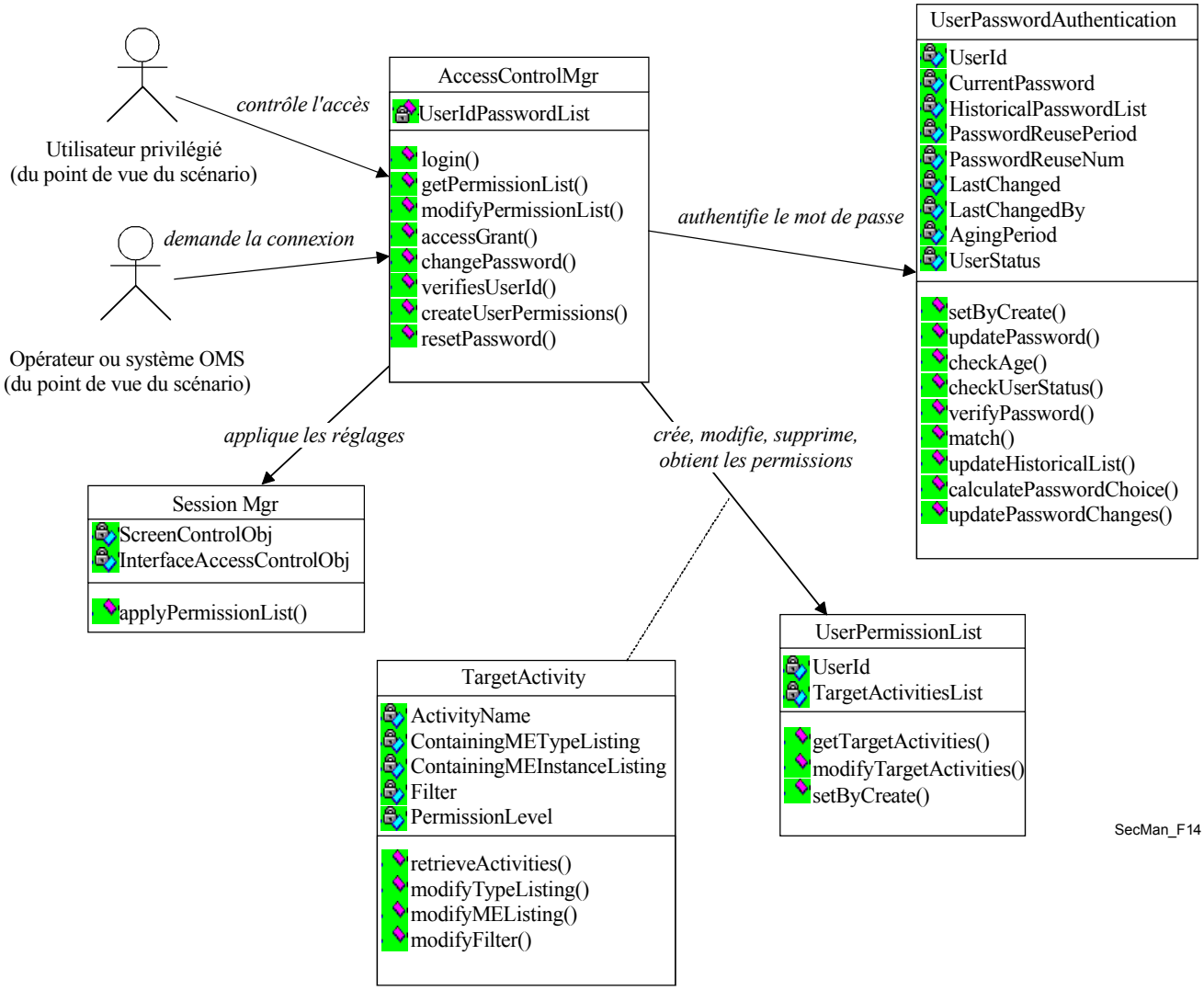


Figure 14
Administration des privilèges des utilisateurs (Q.834.3)

6.4.3 Intersection du plan de gestion et de la couche services

L'intersection entre le plan de gestion et la couche services concerne la sécurisation des activités de surveillance et de contrôle des ressources de réseau configurées pour l'offre de services par le fournisseur de services. Les Recommandations de l'UIT-T portent sur deux aspects de cette intersection. Le premier aspect consiste à veiller à ce que des mesures de sécurité appropriées soient disponibles pour les services qui sont disponibles dans le réseau (par exemple veiller à ce que seuls des utilisateurs valables soient autorisés à exécuter les opérations associées à la fourniture d'un service). Le second aspect consiste à définir les échanges administratifs et de gestion qui sont valables. Cette définition facilitera la détection des violations de sécurité. En cas de violations de sécurité, celles-ci sont souvent gérées au moyen de systèmes de gestion spécifiques.

Un exemple de Recommandation portant sur le premier aspect, l'activité de gestion d'un service, est la Recommandation UIT-T M.3208.2 sur la gestion de connexion. Un client du service de gestion de connexion qui possède des liaisons préconfigurées utilise ce service pour former une connexion par circuits loués de bout en bout. Ce service de gestion de connexion permet à un abonné de créer/activer, modifier et supprimer des circuits loués dans les limites des ressources préconfigurées. Comme l'utilisateur fournit la connectivité de bout en bout, il est nécessaire de garantir que seuls les utilisateurs autorisés peuvent exécuter ces opérations. Les dimensions de sécurité définies pour l'activité de gestion associée à ce service font partie des huit dimensions examinées au 2.5. Ce sont: authentification d'entité homologue, contrôle d'intégrité des données (afin d'empêcher toute modification non autorisée des données en transit) et contrôle d'accès (pour garantir qu'un abonné n'accède pas de façon malveillante ou accidentelle aux données d'un autre abonné).

La Recommandation UIT-T M.3210.1 est un exemple de Recommandation qui définit les activités administratives associées au plan de gestion pour les services hertziens. Elle correspond au second aspect examiné ci-dessus.

Dans un réseau hertzien, lorsque les utilisateurs se déplacent entre leur réseau de rattachement et un réseau visité, ils peuvent traverser différents domaines administratifs. Les services définis dans la Recommandation UIT-T M.3210.1 décrivent comment le domaine de gestion des fraudes du réseau de rattachement collecte les informations appropriées concernant un abonné une fois que celui-ci est enregistré dans un réseau visité. Les scénarios a) et b) de la Figure 15 illustrent le déclenchement de l'activité de gestion de surveillance respectivement par le réseau de rattachement et par le réseau visité.

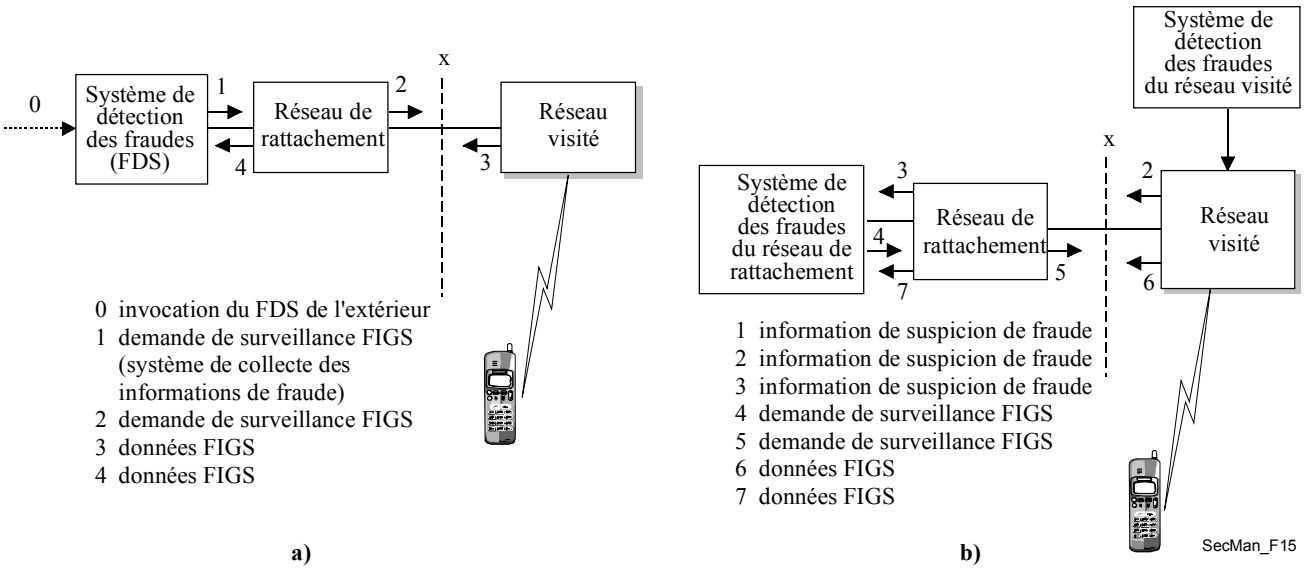


Figure 15
Gestion des fraudes pour les services hertziens (Recommandation M.3210.1)

6.4.4 Intersection du plan de gestion et de la couche application

La troisième cellule, correspondant à l'intersection du plan de gestion et de la couche application, concerne la sécurisation des applications d'utilisateur final fondées sur le réseau. Les applications telles que la messagerie et les services d'annuaire sont définies dans les Recommandations des séries X.400 et X.500.

Une autre catégorie d'applications pour lesquelles les activités de gestion doivent être sécurisées correspond aux applications de gestion proprement dites. Cette déclaration, d'apparence obscure, sera mieux comprise à l'aide d'exemples. Pour ces applications, le personnel de gestion (d'exploitation) faisant partie de l'administration du fournisseur de service représente les utilisateurs finaux. Prenons le cas où un fournisseur de service utilise les services de connexion d'un autre fournisseur pour offrir un service de connectivité de bout en bout. Suivant l'environnement réglementaire ou le marché considéré, certains fournisseurs de services peuvent offrir des services d'accès et d'autres, appelés *opérateurs intercentraux*, peuvent offrir une connectivité longue distance. Les opérateurs intercentraux louent des services d'accès auprès du fournisseur local pour assurer la connectivité de bout en bout entre des endroits géographiques différents. En cas de perte de service, il est fait appel à une application de gestion appelée administration des dossiers de dérangement afin de signaler les dérangements entre systèmes de gestion. L'utilisateur de ces systèmes et de l'application proprement dite a besoin d'une autorisation pour pouvoir signaler des dérangements concernant les services. Les utilisateurs autorisés doivent extraire l'état des dérangements signalés. La Figure 16 illustre les interactions qui doivent être réalisées de manière sécurisée. De manière analogue à l'administration des boîtes vocales pour l'application de messagerie électronique, les privilèges d'accès sont administrés afin d'éviter tout accès non autorisé aux dossiers de dérangement. Un fournisseur de services est autorisé à signaler uniquement des dérangements concernant les services qu'il loue et non des dérangements concernant les services loués par un fournisseur différent.

La Recommandation X.790 définit cette application de gestion et utilise des mécanismes tels que la liste de contrôle d'accès et l'authentification bidirectionnelle pour sécuriser les activités. Cette application a été implémentée et déployée sur la base de cette Recommandation conjointement avec les mécanismes de sécurité applicables à l'authentification.

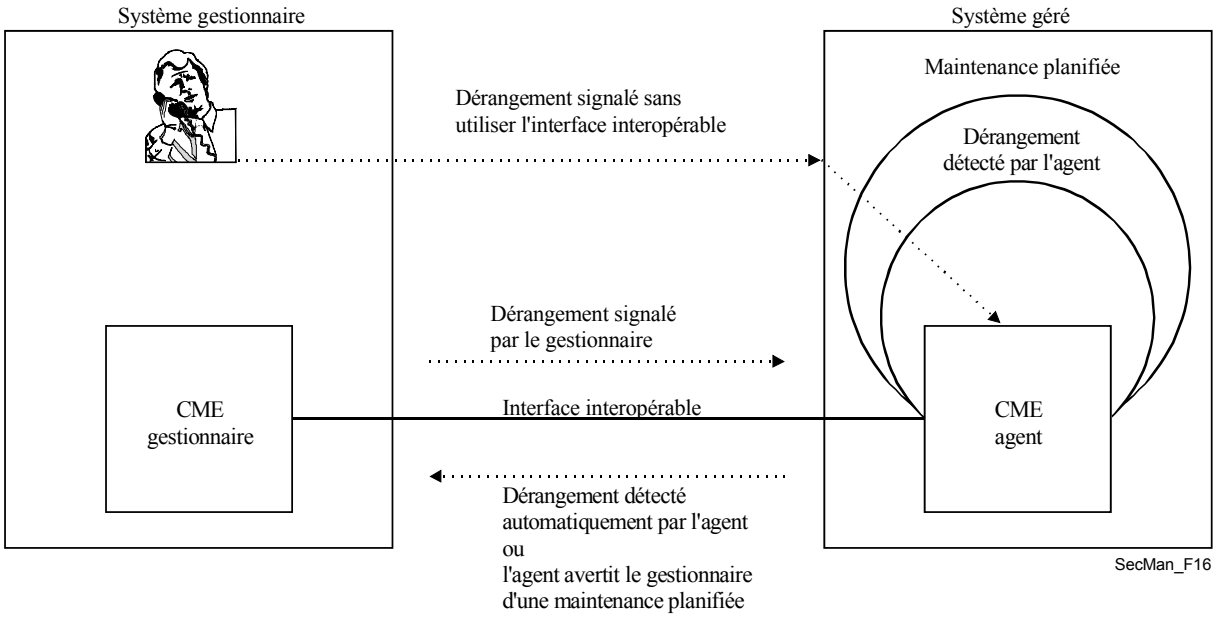


Figure 16
Création d'un dossier de gestion de dérangement (Recommandation UIT-T X.790)

6.4.5 Services communs de gestion de la sécurité

Les Recommandations X.736, X.740 et X.741 définissent des services communs qui s'appliquent aux trois cellules du plan de gestion lorsque le protocole commun d'informations de gestion (CMIP, *common management information protocol*) est utilisé à l'interface. La Recommandation X.736 définit des types d'événement tels que la violation de sécurité physique et les alarmes résultant de ces types d'événement sont signalées aux systèmes de gestion. Il s'agit d'une activité du plan de gestion qui peut être utilisée pour signaler toute violation de sécurité lorsqu'un utilisateur autorisé obtient un accès pour réaliser des activités de configuration dans un élément de réseau ou abonne des utilisateurs à des services ou à des boîtes vocales. La fonction d'audit définie dans la Recommandation X.740 et décrivant la journalisation des événements de violation de sécurité peut être appliquée aux trois couches. La Recommandation X.741 définit un modèle très général et complet permettant d'attribuer des privilèges de contrôle d'accès aux activités de gestion indépendamment des cibles. Le modèle est riche en fonctionnalités, il définit en effet la capacité d'attribuer des privilèges à un niveau élevé de détail des attributs des cibles.

La Recommandation UIT-T Q.816 a par ailleurs adopté les services de sécurité génériques définis par le Forum OMG (*object management group*) pour les activités de gestion réalisées sur la base du modèle CORBA.

6.5 Ordonnances électroniques

La fourniture de soins de santé nécessite et génère une grande variété de données et d'informations, dont la collecte, le traitement, la distribution, l'accès et l'utilisation doivent se faire de façon sécurisée et dans le strict respect des règles éthiques et juridiques. Cela revêt un caractère crucial pour les données cliniques et les informations de gestion, mais est également important pour d'autres types d'informations telles que celles qui sont contenues dans les bases de données épidémiologiques, de littérature et de connaissances.

Les sources de ces types de données et d'informations se trouvent aussi bien à l'intérieur qu'à l'extérieur de l'infrastructure des soins de santé et sont situées à des distances variables de leurs utilisateurs respectifs. En pratique, les utilisateurs nécessitent et génèrent un mélange de ces types d'informations dans le cadre de leurs fonctions respectives, par exemple un médecin peut consulter une base de données de connaissances lorsqu'il examine un patient puis inclure des informations pertinentes dans le dossier du patient, qui peuvent ensuite être utilisées à des fins de facturation.

Les rencontres et les transactions en matière de soins de santé présentent de multiples facettes. Elles se produisent par exemple entre un patient et un médecin, entre deux médecins, entre un médecin généraliste et un médecin spécialiste, entre un patient et un établissement de santé tel qu'un laboratoire d'analyses, une pharmacie ou un centre de rééducation. Ces rencontres peuvent avoir lieu dans sa propre communauté, dans une autre partie du pays ou à l'étranger. Toutes ces rencontres nécessitent des données et des informations avant de commencer véritablement et génèrent des données et des informations en cours de rencontre ou peu après. Ces données et ces informations peuvent être de différentes tailles et être requises ou générées à différents moments et sous différentes formes, par exemple discours, nombres, texte, graphiques et images statiques ou dynamiques, et sont souvent un mélange judicieux de tous ces types.

Les sources et répertoires de ces données et informations peuvent se trouver dans différents endroits et prendre différentes formes, par exemple, dossiers complets des patients, ordonnances écrites à la main et rapports de médecins généralistes, de médecins spécialistes ou de laboratoires.

Traditionnellement, toutes ces rencontres se faisaient en tête-à-tête et les paroles et les écrits étaient les principaux modes utilisés pour les communications et pour l'archivage des dossiers médicaux, tandis que le transport était principalement assuré par des services publics ou privés par voie routière, ferrée ou aérienne. Au fur et à mesure de la croissance du réseau téléphonique, celui-ci est devenu le réseau de communication des professionnels et établissements de santé, à l'échelle nationale et internationale, jusqu'à l'émergence et à la croissance d'outils modernes de télématique pour la santé.

L'utilisation de technologies modernes dans les aspects cliniques/médicaux des services de soins de santé ne fait qu'augmenter et concerne les instruments et les équipements (notamment les équipements de détection et de mesure), les services de laboratoire, l'imagerie statique et dynamique. Compte tenu de la croissance de l'utilisation de ces technologies ainsi que de leur variété et de leur sophistication, il était inévitable que de nombreux services utilisant des technologies modernes se séparent des établissements de soins de santé traditionnels – se séparent sur le plan de la distance et de manière plus significative sur le plan de la gestion. Ainsi, les communications entre ces services utilisant des technologies modernes et les services de soins de santé traditionnels sont devenues importantes du point de vue de l'efficacité et de la rentabilité de ces services.

L'utilisation des technologies de l'information et des communications (TIC) par le secteur de la santé a commencé à se généraliser il y a plus de 25 ans avec la simple messagerie électronique qui permettait d'acheminer des notes et des rapports purement alphanumériques. Tout comme les communications téléphoniques ont constitué le principal motif de l'installation de téléphones dans les cabinets des médecins et dans les établissements de soins de santé, le courrier électronique a été la principale justification initiale de l'installation de liaisons de télécommunication modernes. Et, plus l'utilisation de la messagerie électronique s'est généralisée, plus les exigences en termes de qualité de fonctionnement et de couverture géographique se sont renforcées: davantage d'endroits à une vitesse plus grande et avec une plus grande largeur de bande pour pouvoir prendre en charge les pièces jointes de plus en plus volumineuses des messages électroniques. Au cours des dix dernières années, on a assisté à une croissance exponentielle de l'utilisation de la messagerie électronique dans le secteur de la santé, à l'échelle nationale et internationale, y compris dans les pays les plus pauvres, notamment sur l'Internet. Par exemple, les transactions électroniques sont devenues monnaie courante pour les fonctions qui n'exigent pas vraiment de rencontres en tête-à-tête, par exemple pour préparer et envoyer des ordonnances et des rapports, fixer des rendez-vous et programmer des services, adresser des patients à un confrère et, lorsque la qualité des services de télécommunication le permet, pour transmettre des images médicales accompagnées de leur interprétation écrite ou orale faite par un spécialiste.

Les TIC sont par ailleurs utilisées de façon complexe en télémédecine, qui est "la fourniture de soins médicaux par le biais de communications audio, vidéo et de données", y compris l'établissement effectif du diagnostic, l'examen voire l'apport de soins à un patient qui se trouve dans un endroit distant. La télémédecine est un domaine important qui prend de l'ampleur et qui devrait modifier bon nombre des approches traditionnelles en matière de soins de santé; de fait, c'est le point de départ d'un nouveau modèle pour les soins médicaux.

Un autre domaine qui n'est pas à proprement parler récent, mais qui s'élargira utilement avec la généralisation de la prise en charge de la télématique, est l'accès aux systèmes fondés sur la connaissance et leur utilisation. Ces systèmes, également appelés systèmes experts et systèmes d'appui aux décisions, sont des systèmes qui donnent des avis et conseils spécialisés sur des problèmes et procédures médico-scientifiques. Par exemple, à partir des coordonnées et des symptômes d'un patient, ces systèmes peuvent faciliter l'établissement du diagnostic, suggérer des analyses complémentaires ou proposer un traitement.

Toutes les évolutions susmentionnées ont également une grande incidence sur les systèmes d'informations de gestion (MIS, *management information system*) requis et utilisés dans le secteur de la santé, par exemple les systèmes MIS hospitaliers. Ceux-ci ne sont plus des systèmes destinés à la gestion administrative des soins hospitaliers prodigués aux patients, de l'admission au renvoi/transfert, mais incluent une multitude d'interfaces intelligentes et conviviales pour le personnel médical avec, par exemple, des systèmes d'appui aux décisions cliniques, des liaisons de télémédecine, des portails de sites web, etc.

Par ailleurs, il convient de citer deux caractéristiques des professionnels de santé à prendre en considération: leur mobilité et le besoin qu'ils ont d'avoir les mains libres et donc de pouvoir les utiliser pour les soins médicaux proprement dits. La caractéristique de mobilité signifie qu'ils peuvent accéder aux informations médicales requises (par exemple au dossier électronique d'un patient) ou à un outil ou à un instrument, à partir de n'importe quel endroit distant et chaque fois que c'est nécessaire sous réserve de leur vérification, que ce soit à l'intérieur d'un bâtiment ou d'une ville, mais aussi dans l'ensemble d'un pays ou à l'étranger. Et la caractéristique des mains libres signifie qu'il faut trouver des mécanismes d'identification et d'autorisation qui n'exigent pas d'intervention manuelle du professionnel médical, par exemple ouvrir une porte ou taper sur un clavier d'ordinateur.

Le secteur des soins de santé est donc un secteur fondé sur énormément d'informations, dans lequel la collecte, la circulation, le traitement, la présentation et la distribution de données et d'informations de santé ou liées à la santé, sont essentiels pour l'efficacité, l'efficience et la rentabilité du fonctionnement et du développement des services de soins de santé, à l'échelle nationale et internationale.

Il est extrêmement important que toute cette circulation se fasse de manière sécurisée et confidentielle, et dans le strict respect des règles et réglementations éthiques et juridiques.

6.5.1 Considérations relatives aux infrastructures PKI et PMI pour les applications de télésanté

Par le biais du chaînage des autorités de certification, l'infrastructure PKI reproduit une structure hiérarchique du monde réel, qu'il s'agisse d'une hiérarchie géopolitique (régions-pays-Etats-localités) ou thématique (santé-médecine-chirurgie-chirurgie spécialisée-fournisseurs, etc.). En outre, étant donné que le secteur de la santé est universel, hiérarchique, très important et de plus en plus interactif à l'échelle internationale, la définition d'une interface PKI/PMI normalisée pour la santé devient absolument nécessaire.

L'interopérabilité technique des systèmes de santé doit être garantie grâce à une large utilisation des normes techniques. La plupart des fournisseurs de solutions de sécurité ont déjà adopté des normes telles que la Recommandation UIT-T X.509. L'authentification d'utilisateur étant une application critique qui dépend des informations locales, la liberté de choisir une infrastructure PKI/PMI donnée ne devrait pas avoir d'incidence sur la capacité de l'utilisateur d'interfonctionner avec des personnes certifiées par d'autres infrastructures PKI/PMI dans le secteur de la santé (qui, bien entendu, repose sur au moins un minimum de normalisation concernant les politiques de contrôle d'accès et d'autres politiques associées). Pour cela, différentes stratégies peuvent être mises en place, qui peuvent inclure la reconnaissance croisée des différentes infrastructures ou l'utilisation d'une racine commune. L'adoption de normes techniques, l'interopérabilité technique des différentes infrastructures et la normalisation de certaines politiques garantiront un environnement pleinement efficace et entièrement intégré pour les transactions en matière de santé dans le monde entier.

6.5.2 Système d'ordonnances électroniques de Salford

Le système d'ordonnances électroniques décrit dans le document [Policy] est un bon exemple d'infrastructures PKI et PMI appliquées à la télésanté. Compte tenu du grand nombre de professionnels impliqués dans le programme de transmission électronique des ordonnances (ETP, *electronic transmission of prescriptions*) au Royaume-Uni (34 500 médecins généralistes, 10 000 infirmières délivrant des ordonnances, nombre qui devrait passer à 120 000 au cours des prochaines années, 44 000 pharmaciens agréés et 22 000 dentistes) et des autorisations très peu nombreuses qui sont véritablement requises (c'est-à-dire les divers niveaux de permission concernant la délivrance des ordonnances et des médicaments et l'accès à la gratuité des médicaments), le système de contrôle d'accès en fonction du rôle (RBAC, *role-based access control*) semble constituer le mécanisme

d'autorisation idéal à utiliser pour le programme ETP. Lorsqu'on prend également en considération le nombre de patients potentiels au Royaume-Uni (60 millions) et le fait que les médicaments obtenus gratuitement représentent 85% des médicaments prescrits [FreePresc], le système RBAC devrait aussi être utilisé pour contrôler l'accès à la gratuité des médicaments si possible. Compte tenu du grand nombre de professionnels qui doivent être autorisés et du grand nombre de patients dont l'accès à la gratuité des médicaments doit être accordé, il est essentiel de répartir la gestion des rôles entre autorités compétentes plutôt que d'essayer de la centraliser, faute de quoi le système deviendrait ingérable.

Chaque professionnel dépend d'un organe officiel qui lui donne le droit d'exercer. Au Royaume-Uni, le General Medical Council est chargé d'enregistrer les médecins et de les radier en cas de faute professionnelle. Le General Dental Council remplit une fonction analogue pour les dentistes, le Nursing and Midwifery Council pour les infirmières et le Royal College of Pharmacy pour les pharmaciens. Dans le système ETP susmentionné, ces organes sont chargés de l'attribution des rôles, puisqu'ils s'acquittent déjà parfaitement bien de cette fonction.

Créé en juin 2001, le ministère du travail et des retraites (DWP, *department for work and pensions*) a remplacé les anciens ministères de la sécurité sociale et de l'enseignement et de l'emploi. Il est chargé de verser les allocations de chômage et les retraites et, conjointement avec l'autorité de tarification des ordonnances (PPA, *prescription pricing authority*), de déterminer les bénéficiaires de la gratuité des médicaments. Ces bénéficiaires sont nombreux: personnes de 60 ans et plus, enfants de moins de 16 ans, adolescents de 16, 17 ou 18 ans qui sont scolarisés à temps complet, personnes ou leur conjoint recevant une allocation de soutien du revenu ou une allocation de demandeur d'emploi, personnes titulaires d'un certificat HC2 (*low income scheme full help certificate*) dans le cadre du système de santé national (NHS, *national health system*), femmes enceintes, les femmes ayant accouché au cours des 12 derniers mois et personnes recevant une pension d'invalidité de guerre. La gestion de ces bénéficiaires est donc répartie entre différentes branches du DWP et de la PPA.

Un certificat d'attribut de rôle est attribué à chaque professionnel par l'organe dont il dépend et il est enregistré dans l'annuaire LDAP de cet organe. Le système ETP pourra prendre des décisions concernant l'autorisation de délivrer des ordonnances ou des médicaments s'il a accès à ces annuaires LDAP. De même, si le DWP attribue des certificats d'attribut de rôle aux personnes bénéficiant de la gratuité des médicaments pour diverses raisons et qu'il les enregistre dans son ou ses annuaires LDAP, le système ETP pourra prendre des décisions concernant l'accès à la gratuité des médicaments en accédant à ces annuaires LDAP, et le pharmacien n'aura pas à demander au patient la preuve qu'il bénéficie de cette gratuité. Cette preuve ne sera nécessaire que lorsqu'un patient fait nouvellement partie des bénéficiaires, par exemple lorsque la grossesse d'une femme vient tout juste d'être diagnostiquée par son médecin généraliste et que le DWP n'a pas eu le temps de créer le certificat d'attribut officiel.

Ces rôles sont ensuite utilisés par un moteur de décision (tel que PERMIS, voir www.permis.org), qui détermine si des médecins sont autorisés à délivrer des ordonnances, des pharmaciens à délivrer des médicaments et des patients à bénéficier de la gratuité des ordonnances, conformément à la politique ETP. Chaque application ETP (système pour la délivrance des ordonnances, système pour la délivrance des médicaments et système PPA) lit la politique ETP au moment de l'initialisation puis, lorsqu'un professionnel demande une action (par exemple délivrer une ordonnance ou des médicaments), le moteur de décision extrait le rôle de la personne dans l'annuaire LDAP approprié et prend une décision conformément à la politique. Les utilisateurs peuvent donc accéder à de multiples applications et tout ce dont ils ont besoin d'avoir est une paire de clés PKI. L'émission des certificats d'attribut de rôle peut avoir lieu sans que l'utilisateur n'intervienne et les utilisateurs n'ont pas à se soucier de savoir comment et où ces certificats sont enregistrés et utilisés par le système.

La Figure 17 contient un exemple d'implémentation d'un système d'ordonnances électroniques au Royaume-Uni, qui illustre plusieurs problèmes de sécurité essentiels qui se posent au moment de l'implémentation. Le cœur du système est constitué par une infrastructure de sécurité qui assure non seulement une forte authentification (à savoir une infrastructure PKI utilisant des certificats de clé publique) mais aussi une forte autorisation (à savoir une infrastructure PMI) qui permet de donner une autorisation aux professionnels médicaux sur la base de leurs rôles enregistrés dans les certificats d'attribut. Les modèles classiques utilisent des listes de contrôle d'accès enfouies dans chaque application particulière (par exemple dossiers médicaux, bases de données d'ordonnances, assurance, etc.), pouvant obliger les utilisateurs (médecins, pharmaciens, patients, etc.) à obtenir et à administrer plusieurs jetons de sécurité différents (par exemple nom d'utilisateur/mot de passe, carte, etc.). Dans le nouveau modèle qui intègre les architectures PKI et PMI, l'utilisateur n'a besoin que d'un seul jeton – le certificat de clé publique de l'utilisateur – pour accéder aux différents services et aux différentes ressources qui sont réparties géographiquement ou topologiquement. Les certificats d'attribut de l'utilisateur sont conservés dans le système et non par l'utilisateur et sont transférés d'un composant à un autre en fonction des souhaits afin d'accorder un accès. Comme les certificats d'attribut sont signés numériquement par leurs émetteurs, ils ne peuvent pas être altérés au cours de ces transferts.

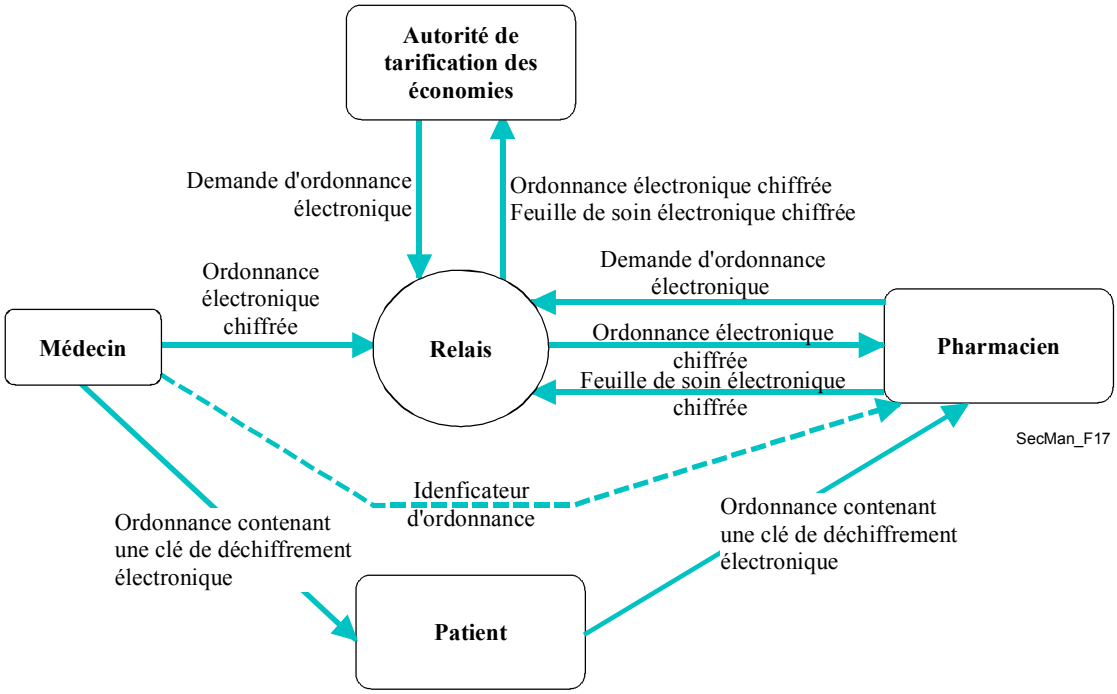


Figure 17
Système d'ordonnances électroniques de Salford

Dans l'exemple de la Figure 17, des ordonnances électroniques sont créées par le médecin, signées numériquement (à des fins d'authentification), soumises à un chiffrement symétrique au moyen d'une clé de session aléatoire (à des fins de confidentialité), puis envoyées à une unité de stockage centrale. Le patient reçoit une ordonnance papier sur laquelle figure un code barre contenant la clé de chiffrement symétrique. Il se rend ensuite à la pharmacie de son choix et remet l'ordonnance au pharmacien, qui scanne le code barre, extrait l'ordonnance et la déchiffre. C'est le patient qui, en fin de compte, a la maîtrise de la personne qui est autorisée à lui délivrer les médicaments, comme dans le système actuel fonctionnant avec des ordonnances papier. Mais ce n'est pas suffisant. Il faut également prévoir des contrôles concernant les personnes autorisées à prescrire tel ou tel médicament et les personnes autorisées à les délivrer et concernant les personnes bénéficiant de la gratuité des médicaments.

Même si la description ci-dessus fait apparaître un système fortement intégré, celui-ci peut en réalité être réparti. En effet, l'annuaire d'attributs des médecins peut être différent du système qui authentifie les pharmaciens ou qui stocke les droits et politiques en matière de délivrance de médicaments, etc., qui s'appuient sur des tiers de confiance pour authentifier et autoriser les différents acteurs. Même si la mise en œuvre de solutions propriétaires est envisageable pour les infrastructures PKI et PMI, le recours à des solutions normalisées (par exemple la Recommandation UIT-T X.509) permet aujourd'hui d'offrir un accès plus généralisé et global aux ordonnances électroniques.

7 Conclusions

L'UIT-T a commencé il y a longtemps à élaborer un ensemble de Recommandations fondamentales sur la sécurité: X.800 est un document de référence sur l'architecture de sécurité pour l'interconnexion des systèmes ouverts et la série X.810-X.816 définit un cadre de sécurité pour les systèmes ouverts, les Recommandations de cette série traitant respectivement de l'aperçu général, de l'authentification, du contrôle d'accès, de la non-répudiation, de la confidentialité, de l'intégrité et enfin de l'audit et des alarmes de sécurité. Plus récemment, la Recommandation UIT-T X.805 a été élaborée en vue de décrire l'architecture de sécurité pour les systèmes assurant des communications de bout en bout. La modification architecturale que la Recommandation X.805 représente tient compte des menaces et vulnérabilités plus nombreuses qui résultent d'un environnement devenu multiréseaux et multifournisseurs de services. La Recommandation X.509 portant sur le cadre général des certificats de clé publique et d'attribut est certainement le texte de l'UIT-T auquel il est le plus souvent fait référence en matière d'applications de sécurité, soit directement, soit implicitement dans d'autres normes reposant sur les principes énoncés dans la Recommandation X.509.

En plus de ces Recommandations cadres, l'UIT-T a établi des dispositions relatives à la sécurité de plusieurs systèmes et services définis dans ses Recommandations. Le paragraphe 6 du présent manuel décrit notamment les applications suivantes: téléphonie IP utilisant H.323 ou IPCablecom, transmission sécurisée de télécopie et gestion de réseau. Il donne également un exemple d'application des infrastructures de clé publique et de gestion de privilège à la télésanté. Il convient de noter qu'il existe de nombreux *autres* domaines dans lesquels les besoins de sécurité sur le plan des télécommunications et des technologies de l'information sont pris en considération dans les Recommandations de l'UIT-T. Ces domaines et des aspects tels que la prévention des fraudes, le rétablissement et le retour à la normale après une catastrophe, examinés au sein de plusieurs Commissions d'études de l'UIT-T, seront abordés dans de futures éditions. A l'appui de ses travaux sur la sécurité, l'UIT-T organise ou participe à des séminaires ou ateliers internationaux sur la sécurité, élabore un projet de sécurité et a désigné une commission d'études directrice pour les travaux de l'UIT-T sur la sécurité.

Références

En plus des Recommandations de l'UIT-T (qui figurent à l'adresse www.itu.int/ITU-T/publications/recs.html) mentionnées dans le présent manuel, les documents suivants ont également été utilisés.

[ApplCryp] B. Schneier, "Applied Cryptography – Protocols, Algorithms and Source Code in C" (*Cryptographie appliquée – protocoles, algorithmes et code source en C*) 2ème édition, Wiley, 1996; ISBN 0-471-12845-7

[Chadwick] D. W. Chadwick; "The Use of X.509 in E-Healthcare" (*Utilisation de la Recommandation X.509 dans le domaine de la télésanté*) , atelier sur la normalisation dans le domaine de la télésanté; Genève, 23-25 mai 2003; fichier PowerPoint à l'adresse www.itu.int/itudoc/itu-t/workshop/e-health/s5-02.html et présentation audio à l'adresse www.itu.int/ibs/ITU-T/e-health/Links/B-20030524-1100.ram

[Euchner] M. Euchner, P-A. Probst; "Multimedia Security within Study Group 16: Past, Presence and Future" (*Sécurité des systèmes multimédias au sein de la Commission d'études 16: passé, présent et avenir*) , atelier de l'UIT-T sur la sécurité; 13-14 mai 2002, Séoul, Corée; www.itu.int/itudoc/itu-t/workshop/security/present/s2p3r1.html

[FreePresc] Statistiques relatives à la gratuité des médicaments au Royaume-Uni; www.doh.gov.uk/public/sb0119.htm

[Packetizer] "A Primer on the H.323 Series Standard" (*Contribution sur la norme H.323*) www.packetizer.com/iptel/h323/papers/primer/

[Policy] D. W. Chadwick, D. Mundy; "Policy Based Electronic Transmission of Prescriptions" (*Transmission électronique des ordonnances fondée sur des politiques*); IEEE POLICY 2003, 4-6 juin, lac de Côme, Italie. sec.isi.salford.ac.uk/download/PolicyBasedETP.pdf

[SG17] Commission d'études 17 de l'UIT-T; "Commission d'études directrice pour la sécurité des systèmes de communication" www.itu.int/ITU-T/studygroups/com17/cssecurity.html (*paragraphe 2* portant sur le catalogue des Recommandations de l'UIT-T relatives à la sécurité des systèmes de communication; *paragraphe 3* portant sur le recueil des définitions relatives à la sécurité figurant dans les Recommandations de l'UIT-T)

[Shannon] G. Shannon; "Security Vulnerabilities in Protocols" (*Vulnérabilités de sécurité dans les protocoles*); atelier de l'UIT-T sur la sécurité; 13-14 mai 2002, Séoul, Corée; www.itu.int/itudoc/itu-t/workshop/security/present/s1p2.html

[Wisekey] S. Mandil, J. Darbellay; "Public Key Infrastructures in e-health" (*Infrastructures de clé publique dans le domaine de la télésanté*); contribution écrite à l'atelier sur la normalisation dans le domaine de la télésanté; Genève, 23-25 mai 2003; www.itu.int/itudoc/itu-t/workshop/e-health/wcon/s5con002_ww9.doc

Annexe A: Terminologie dans le domaine de la sécurité

Les acronymes et termes suivants sont extraits de Recommandations de l'UIT-T et d'autres sources externes, comme indiqué ci-dessous. Des sources complémentaires sont présentées au paragraphe A.3 de la présente Annexe.

A.1 Acronymes relatifs à la sécurité fréquemment utilisés

Acronyme	Définition
3DES	[H.235] Triple DES (*triple DES*)
A	[M.3010] Agent (*agent*)
A/M	[M.3010] Agent/gestionnaire (*agent/manager*)
AA	[X.509] Autorité d'attribut (*attribute authority*)
AAA	[X.805] Authentification, autorisation et comptabilité (*authentication, authorization and accounting*)
AARL	[X.509] Liste de révocation d'autorité d'attribut (*attribute authority revocation list*)
ACI	[X.810] Information de contrôle d'accès (*access control information*)
ACRL	[X.509] Liste de révocation de certificat d'attribut (*attribute certificate revocation list*)
AE	[M.3010] Entité d'application (*application entity*)
AES	[H.235] [J.170] Norme de chiffrement perfectionné (*advanced encryption standard algorithm*)
AH	[J.170] L'en-tête d'authentification (*authentication header*) est un protocole de sécurité IPSec qui assure l'intégrité des paquets IP complets, y compris l'en-tête IP.
ASCII	[T.36] American Standard Code for Information Interchange
ASD	[J.170] Données propres à l'application (*application-specific data*). Il s'agit d'un champ propre à l'application figurant dans l'en-tête IPSec qui, conjointement avec l'adresse IP de destination, constitue un nombre unique pour chaque association de sécurité (SA)
ASN.1	[X.680] Notation de syntaxe abstraite numéro un (*abstract syntax notation no.1*)
ASP	[X.805] Fournisseur de services d'applications (*application service provider*)
ATM	[X.805] Mode de transfert asynchrone (*asynchronous transfer mode*)
ATM	[M.3010] Mode de transfert asynchrone (*asynchronous transfer mode*)
AuF	[H.530] Fonction d'authentification (*authentication function*), voir la Rec. UIT-T H.510 [6]
B(n)	[T.36] Valeur de base (n) (*base value (n)*)
BE	[H.530] Elément frontière (*border element*), voir l'Annexe G de la Rec. UIT-T H.225.0 [2]
BES	[H.235] Serveur d'arrière (*backend server*)
BML	[M.3010] Couche de gestion d'entreprise (*business management layer*)
B-OSF	[M.3010] Fonction de système d'exploitation – Couche de gestion d'entreprise (*business management layer – operations systems function*)
BPI+	[J.170] L'interface de base pour le respect de la vie privée plus (*baseline privacy interface plus*) est la partie sécurité de la norme J.112 s'appuyant sur la couche MAC.
CA	[H.234] [H.235] [J.170] [X.509] Autorité de certification (*certification authority*). Il s'agit d'une organisation de confiance qui accepte les demandes de certificat provenant des entités, authentifie les demandes, émet les certificats et tient à jour les informations d'état concernant les certificats. [J.170] agent d'appel (*call agent*). Il s'agit de la partie du serveur CMS qui maintient l'état de communication et contrôle le côté ligne de la communication.
CARL	[X.509] Liste de révocation d'autorité de certification (*certification authority revocation list*)
CBC	[H.235] [J.170] Chiffrement en mode chaînage de blocs (*cipher block chaining*)
CCA	[H.234] Autorité de certification de pays (*country certification authority*)
CFB	[H.235] Chiffrement en mode rétroaction (*cipher feedback mode*)
CH_n	[H.530] Epreuve numéro n (*challenge number n*)

Acronyme	Définition
CM	[J.170] Câblomodem (*cable modem*)
CME	[X.790] Entité de gestion conforme (*conformant management entity*)
CMIP	[M.3010] Protocole commun d'informations de gestion (*common management information protocol*)
CMIS	[X.790] Service commun d'informations de gestion (*common management information service*)
CMISE	[X.790] Elément du service commun d'informations de gestion (*common management information service element*)
CMS	[J.170] Syntaxe des messages cryptographiques (*cryptographic message syntax*). [J.170] Serveur de gestion d'appels (*call management server*), qui contrôle les connexions audio. Également appelé agent d'appel dans la terminologie MGCP/SGCP (c'est un exemple de serveur d'application).
CMTS	[J.112] Système de terminaison de câblomodem (*cable modem termination system*)
CNM	[X.790] Gestion de réseau client (*customer network management*)
CORBA	[SANCHO] Architecture de courtier commun de requêtes d'objets (*common object request broker architecture*)
CRL	[H.235] [X.509] Liste de révocation de certificat (*certificate revocation list*)
DCF	[M.3010] Fonction de communication de données (*data communication function*)
dCRL	[X.509] Liste delta de révocation de certificat (*delta certificate revocation list*)
DES	[H.235] [J.170] Norme de chiffrement des données (*data encryption standard*)
DH	[H.235] [H.350] Diffie-Hellman
DHCP	[J.170] [X.805] Protocole de configuration de serveur dynamique (*dynamic host configuration protocol*)
DIB	[X.509] Base d'informations d'annuaire (*directory information base*)
DIT	[X.509] Arbre d'informations d'annuaire (*directory information tree*)
DN	[X.790] Nom distinctif (*distinguished name*)
DNS	[H.235] [J.170] [X.805] Serveur de noms de domaine (*domain name server*)
DOCSIS	[J.170] Spécification d'interface du service de transmission de données par câble (*data-over-cable service interface specification*)
DoS	[X.805] Déni de service (*denial of service*)
DQoS	[J.170] Qualité de service dynamique (*dynamic quality of service*)
DS-3	[X.805] Signal numérique de niveau 3 (*digital signal level 3*)
DSA	[X.509] Agent de système d'annuaire (*directory system agent*)
DSCP	[J.170] Point de code des services différenciés (*diffserv code point*). Il s'agit d'un champ dans chaque paquet IP qui identifie le comportement des services différenciés pour chaque bond. Dans la version 4 du protocole IP, l'octet TOS est redéfini comme étant le champ DSCP. Dans la version 6 du protocole IP, l'octet de classe de trafic est utilisé comme champ DSCP. Voir l'Annexe C.
DSS	[H.235] Norme de signature numérique (*digital signature standard*)
DTMF	[H.235] [J.170] (tonalités) Multifréquence bitonalités (*dual-tone multi frequency*)
DUA	[X.509] Agent d'utilisateur d'annuaire (*directory user agent*)
EARL	[X.509] Liste de révocation de certificat d'attribut d'entité finale (*end-entity attribute certificate revocation list*)
ECB	[H.235] Chiffrement en mode dictionnaire (*electronic code book mode*)
ECC, EC	[H.235] Système cryptographique à courbe elliptique (*elliptic curve cryptosystem*) (voir le 8.7 de la version 1.1 de la spécification de sécurité de l'ATM Forum). Il s'agit d'un système cryptographique à clé publique.

Acronyme	Définition
EC-GDSA	[H.235] Signature numérique à courbe elliptique avec appendice analogue à l'algorithme de signature numérique NIST (DSA) (*elliptic curve digital signature with appendix analog of the NIST digital signature algorithm (DSA)*) (voir aussi la norme [ISO/CEI 15946-2, chapitre 5])
ECKAS-DH	[H.235] Système de concordance de clés à courbe elliptique – Diffie-Hellman (*elliptic curve key agreement scheme – Diffie-Hellman*). Il s'agit du système de concordance de clés de Diffie-Hellman utilisant la cryptographie à courbe elliptique.
EML	[M.3010] Couche de gestion d'élément (*element management layer*)
EOFB	[H.235] chiffrement en mode OFB amélioré (*enhanced OFB mode*)
E-OSF	[M.3010] Fonction de système d'exploitation – couche de gestion d'élément (*element management layer – operations systems function*)
EP	[H.235] Point d'extrémité (*endpoint*)
EP_{ID}	[H.530] Identificateur de point d'extrémité MT (*MT endpoint identifier*), voir la Rec. UIT-T H.225.0 [1]
EPRL	[X.509] Liste de révocation de certificat de clé publique d'entité finale (*end-entity public-key certificate revocation list*)
ESH	[T.36] Valeur de hachage chiffrée et embrouillée (*encrypted and scrambled plain hash*) (24 chiffres décimaux)
ESIM	[T.36] Message d'intégrité embrouillé et chiffré (*encrypted scrambled integrity message*). Nombre de 12 chiffres décimaux.
ESP	[J.170] Sécurité d'encapsulation IPSec (*ipsec encapsulating security*)
ESSK	[T.36] Clé secrète embrouillée et chiffrée (*encrypted scrambled secret key*). Nombre de 12 chiffres décimaux.
FDS	[M.3210.1] Système de détection des fraudes (*fraud detection system*)
FEAL	[T.36] L'algorithme de chiffrement de données rapide (*fast data encipherment algorithm*) est une famille d'algorithmes qui convertit chaque bloc de texte en clair de 64 bits en un bloc de texte chiffré de 64 bits à l'aide d'une clé secrète de 64 bits. Il est analogue à l'algorithme DES mais comporte une fonction f beaucoup plus simple. Il a été conçu pour être rapide et simple, afin d'être adapté aux microprocesseurs peu complexes (par exemple les cartes à puce). (voir A. Menezes et al., Handbook of Applied Cryptography, CRC Press, 1997).
FIGS	[M.3210.1] Système de collecte des informations de fraude (*fraud information gathering system*)
FQDN	[J.170] Nom de domaine entièrement qualifié (*fully qualified domain name*). Voir le document RFC 821 de l'IETF pour plus de détails.
FTP	[X.805] Protocole de transfert de fichiers (*file transfer protocol*)
FU	[X.790] Unité fonctionnelle (*functional unit*)
GCA	[H.234] Autorité de certification générale (*general certification authority*)
GDMI	[M.3210.1] Directives pour la définition des interfaces de gestion RGT (*guidelines for the definition of TMN management interface*)
GDMO	[M.3010] Directives pour la définition des objets gérés (*guidelines for the definition of managed objects*)
GK	[H.235] [H.510] [H.530] Portier (*gatekeeper*)
GK_{ID}	[H.530] Identificateur de portier du domaine visité (*visited gatekeeper identifier*), voir la Rec. UIT-T H.225.0 [1]
GNM	[X.790] Modèle de réseau général (*general network model*)
GRJ	[H.530] Refus de portier (*gatekeeper reject*)
GRQ	[H.530] Demande de portier (*gatekeeper request*)
GW	[H.235] Passerelle (*gateway*)
h[*]	[H.234] Résultat de la fonction h appliquée à *
H-BE	[H.530] Elément frontière du domaine de rattachement (*home BE*)

Acronyme	Définition
HFC	[J.165] Système hybride fibre optique/câble coaxial (*hybrid fibre/coaxial*)
HFX	[T.30] [T.36] Chiffrement de télécopie de Hawthorne (*hawthorne facsimile cipher*)
H-GK	[H.530] Portier du domaine de rattachement (*home GK*)
HKM	[T.30] [T.36] Algorithme de gestion de clés de Hawthorne (*hawthorne key management algorithm*)
HKMD1	[T.36] Double chiffrement utilisant l'algorithme HKM (*double encryption using the HKM algorithm*)
HLF	[H.530] Fonction de localisation dans le domaine de rattachement (*home location function*)
HMAC	[J.170] Code d'authentification de message haché (*hashed message authentication code*). Algorithme d'authentification de message, fondé sur l'algorithme de hachage SHA-1 ou MD-5 et défini dans le document RFC 2104.
HMAC-SHA1-96	[H.530] Code d'authentification de message haché avec l'algorithme 1 de hachage sécurisé
$HMAC_Z$	[H.530] Code/réponse d'authentification de message haché par clé avec secret partagé Z, si Z n'est pas montré, on applique le secret lié au bond suivant.
iCRL	[X.509] Liste indirecte de révocation de certificat (*indirect certificate revocation list*)
ICV	[H.235] Valeur de contrôle d'intégrité (*integrity check value*)
ID	[H.235] Identificateur (*identifier*)
IDEA	[T.36] L'algorithme international de chiffrement de données (*international data encryption algorithm*) est un algorithme de chiffrement créé par Xuejia Lai et James Massey en 1992 qui utilise un chiffrement par blocs avec une clé de 128 bits (blocs de 64 bits avec une clé de 128 bits) et qui est généralement considéré comme étant très sûr. Il est considéré comme faisant partie des meilleurs algorithmes publics. Pendant les quelques années au cours desquelles il a été utilisé, aucune attaque véritable n'a été signalée malgré un grand nombre de tentatives (http://searchsecurity.techtarget.com/gDefinition/0,294236,sid14_gci213675,00.html).
Idx	[T.36] Six derniers chiffres de l'identification télécopieur (numéro de téléphone pour la télécopie) de X
Idy	[T.36] Six derniers chiffres de l'identification télécopieur (numéro de téléphone pour la télécopie) de Y
IKE	[J.170] L'échange de clés Internet (*internet key exchange*) est un mécanisme de gestion de clés utilisé pour négocier et obtenir des clés pour des associations de sécurité (SA) dans le protocole IPSec.
IKE–	[J.170] Notation désignant l'utilisation du mécanisme IKE avec des clés préalablement partagées pour l'authentification.
IM	[T.36] Message d'intégrité (*integrity message*) servant à confirmer ou à réfuter l'intégrité du message reçu (12 chiffres décimaux)
IMT-2000	[M.3210.1] Télécommunications mobiles internationales 2000 (*international mobile telecommunications 2000*)
IMy	[T.36] Message d'intégrité (*integrity message*) émis par Y pour confirmer ou réfuter l'intégrité du message reçu. Nombre de 12 chiffres décimaux.
IP	[X.805] Protocole Internet (*internet protocol*)
IPSec	[H.235] [H.530] [J.170] [X.805] Sécurité du protocole Internet (*internet protocol security*).
ISAKMP	[H.235] Protocole de gestion de clé pour les associations de sécurité Internet (*internet security association key management protocol*)
ISTP	[J.170] Protocole de transport de signalisation Internet (*internet signalling transport protocol*)
IV	[H.235] Vecteur d'initialisation (*initialization vector*)
IVR	[J.170] Système à réponse vocale interactive (*interactive voice response system*)
K	[H.530] Clé de session/liaison dynamique (*dynamic session/link key*)

Acronyme	Définition
KDC	[J.170] Centre de distribution de clés (*key distribution center*)
LAN	[M.3010] Réseau local (*local area network*)
LDAP	[H.235] Protocole rapide d'accès à l'annuaire (*lightweight directory access protocol*)
LLA	[M.3010] Architecture logique répartie en couches (*logical layered architecture*)
MAC	[H.235] [J.170] Code d'authentification de message (*message authentication code*). Il s'agit d'un élément de données de longueur fixe qui est envoyé conjointement avec un message pour en garantir l'intégrité, également appelé MIC. [J.170] Commande d'accès au support (*media access control*). C'est une sous-couche de la couche liaison de données. Elle se trouve normalement directement au-dessus de la couche physique.
MAF	[M.3010] Fonction d'application de gestion (*management application function*)
MAN	[M.3010] Réseau métropolitain (*metropolitan area network*)
MAPDU	[X.790] Unité de données de protocole d'application de gestion (*management application protocol data unit*)
MCU	[H.235] Unité de multidiffusion. [H.323] Pont de conférence/unité de commande multipoint (*multipoint control unit*)
MD-5	[H.235] [J.170] Condensé de message N° 5 (*message digest no. 5*)
MG	[J.170] Passerelle média (*media gateway*).
MGC	[J.170] Contrôleur de passerelle média (*media gateway controller*).
MGCP	[J.170] Protocole de commande de passerelle média (*media gateway control protocol*).
MIB	[J.170] [M.3010] Base d'informations de gestion (*management information base*)
MIS	[M.3010] Service d'informations de gestion (*management information service*)
MO	[M.3010] Objets gérés (*managed objects*)
mod n	[T.36] Opérateur modulo utilisant la base n
MPS	[H.235] Flux de charges utiles multiples (*multiple payload stream*)
MPx	[T.36] Primitive mutuelle de X (*mutual primitive of X*). Nombre de 16 chiffres décimaux, qui ne peut être créé que par X au moyen de l'algorithme HKM et des primitives formées avec UINx, UCNx, IDx et Idy.
MPy	[T.36] Primitive mutuelle de Y (*mutual primitive of Y*)
MRP	[H.530] Proxy de routage pour la mobilité (*mobility routing proxy*)
MS	[M.3210.1] Services de gestion (*management services*)
MSB	[J.170] Bit le plus significatif (*most significant bit*)
MT	[H.530] Terminal mobile (*mobile terminal*), voir la Rec. UIT-T H.510 [6]
MTA	[J.170] Adaptateur de terminal média (*media terminal adapter*).
NAT	[H.235] Traduction d'adresse de réseau (*network address translation*)
NCS	[J.170] Signalisation d'appel par le réseau (*network call signalling*)
NE	[M.3010] [X.790] Elément de réseau (*network element*)
NEF	[M.3010] Fonction d'élément de réseau (*network element function*)
NEF-MAF	[M.3010] Fonction d'élément de réseau – Fonction d'application de gestion (*network element function – management application function*)
NML	[M.3010] [M.3210.1] Couche de gestion de réseau (*network management layer*)
NOC	[X.790] Centre d'exploitation de réseau (*network operations centre*)
N-OSF	[M.3010] Fonction de système d'exploitation – Couche de gestion de réseau (*network management layer – operations systems function*)
NTP	[H.530] Protocole relatif au temps dans le réseau (*network time protocol*)
O	[M.3010] Optionnel (*optional*)

Acronyme	Définition
OA&M	[M.3010] Exploitation, administration et maintenance (*operations, administration and maintenance*)
OAM&P	[SANCHO] Exploitation, administration, maintenance et fourniture (*operations, administration, maintenance & provisioning*)
OCSP	[H.235] Protocole de statut de certificat en ligne (*online certificate status protocol*)
ODP	[X.810] Traitement réparti ouvert (*open distributed processing*)
OFB	[H.235] Chiffrement en mode rétroaction de sortie (*output feedback mode*)
OID	[H.235] [H.530] [J.170] [M.3010] Identificateur d'objet (*object identifier*)
OS	[M.3010] [X.790] Système d'exploitation (*operations system*)
OSF	[M.3010] Fonction de système d'exploitation (*operations systems function*)
OSF-MAF	[M.3010] Fonction de système d'exploitation – Fonction d'application de gestion (*operations systems function – management application function*)
OSI	[M.3010] [X.790] [X.805] [X.810] Interconnexion des systèmes ouverts (*open systems interconnection*)
OSS	[J.170] Système d'assistance à l'exploitation (*operations systems support*). Il s'agit des logiciels d'arrière utilisés pour la gestion de la configuration, de la qualité de fonctionnement, des défauts, de la comptabilité et de la sécurité.
OT	[T.36] Clé à usage unique (*one-time key*). Nombre de 6 à 64 chiffres décimaux défini par les deux utilisateurs.
OTx	[T.36] Clé à usage unique utilisée en premier par X lors de son enregistrement auprès de Y
OTy	[T.36] Clé à usage unique utilisée en premier par Y lorsque celui-ci s'enregistre auprès de X en vue de l'enregistrement mutuel, cette clé pouvant être différente ou non d'OTx
P(n)	[T.36] Valeur de phase (n) (*phase value (n)*)
PBX	[M.3010] Autocommutateur privé (*private branch exchange*)
PDU	[H.235] Unité de données de protocole (*protocol data unit*)
PH	[T.36] Valeur de hachage du message (24 chiffres décimaux) (*plain hash*)
PKCROSS	[J.170] Utilise PKINIT pour établir les clés inter-secteurs et les politiques associées intersecteurs à appliquer pour émettre des tickets de service transsecteurs entre secteurs et domaines à l'appui de la signalisation entre serveurs CMS (CMSS) intradomaine ou interdomaines.
PKCS	[H.235] [J.170] [X.509] Normes de chiffrement par clé publique (*public key cryptography standards*)
PKI	[H.235] [H.530] [X.509] [J.170] Infrastructure de clé publique (*public key infrastructure*). Processus permettant d'émettre des certificats de clé publique, incluant des normes, des autorités de certification, une communication entre autorités et des protocoles de gestion des processus de certification.
PMI	[X.509] Infrastructure de gestion de privilège (*privilege management infrastructure*)
PRF	[H.235] Fonction pseudo-aléatoire (*pseudo-random function*)
Primitive	[T.36] Nombre composé de 64 chiffres formé à partir de UIN et de UCN
procREGxy	[T.36] Procédure d'enregistrement entre X et Y
procSTKxy	[T.36] Procédure permettant à X de procéder à la transmission sécurisée d'une clé secrète à Y
PRS	[T.36] Séquence pseudo-aléatoire (*pseudorandom sequence*)
PTO	[M.3010] Opérateur de télécommunications publiques (*public telecommunication operator*)
PTR	[X.790] Dossier de dérangement de fournisseur (*provider trouble report*)
PVC	[X.805] Circuit virtuel permanent (*permanent virtual circuit*)
PW	[H.530] Mot de passe d'utilisateur mobile (*mobile user password*)
QA	[M.3010] Adaptateur Q (*Q adapter*)
QoS	[SANCHO] Qualité de service (*quality of service*)

Acronyme	Définition
R	[M.3010] Ressource (*resource*)
R_1	[H.530] Nombre aléatoire (*random number*)
RADIUS	[J.170] Service utilisateur d'authentification par téléphone (*remote authentication dial-in user service*)
RBAC	[X.509] Contrôle d'accès en fonction du rôle (*role-based access control*)
RC4	[J.170] Chiffrement de flux à clé de longueur variable offert dans une suite de chiffrement et servant à chiffrer le trafic de média dans le système IPCablecom.
RCD	[M.3010] Réseau de communication de données
RCN	[T.36] Nombre crypté enregistré. Nombre de 16 chiffres décimaux (*registered crypt number*).
RDN	[X.790] Nom distinctif relatif (*relative distinguished name*)
RGT	[M.3010] [M.3210.1] [X.790] Réseau de gestion des télécommunications
RI	[M.3010] Réseau intelligent
RIP	[H.530] Demande en cours (*request in progress*)
RKS	[J.170] Serveur d'archivage (*record keeping server*). Dispositif qui collecte et corrèle les divers messages d'événement.
RNCn	[T.36] Nombre aléatoire non secret associé à une clé SCn. Nombre de 4 chiffres décimaux (*non-secret random number associated with an SCn*)
RNIM	[T.36] Nombre aléatoire non secret associé à un message IM. Nombre de 4 chiffres décimaux (*non-secret random number associated with an IM*)
RNIS	[M.3010] Réseau numérique à intégration de services
RNK	[T.36] Nombre aléatoire non secret permettant de faire varier les primitives créées par MPx lors du chiffrement d'une clé SK. Nombre de 4 chiffres décimaux.
RNSRn	[T.36] Nombre aléatoire non secret associé à une clé SRn. Nombre de 4 chiffres décimaux.
RNSSn	[T.36] Nombre aléatoire non secret associé à une clé SSn. Nombre de 4 chiffres décimaux.
RRJ	[H.530] Refus d'enregistrement (*registration reject*)
RRQ	[H.530] Demande d'enregistrement (*registration request*)
RSA	[H.235] [T.30] [T.36] Rivest, Shamir et Adleman (algorithme à clé publique)
RSVP	[J.170] Protocole de réservation de ressource (*resource reservation protocol*)
RTCP	[H.235] [J.170] Protocole de commande de transport en temps réel (*realtime transport control protocol*)
RTO	[J.170] Temporisation de retransmission (*retransmission timeout*)
RTP	[H.225.0] [H.235] [J.170] Protocole de transport en temps réel (*real time protocol*)
RTPC	[SANCHO] Réseau téléphonique public commuté
SA	[J.170] Association de sécurité (*security association*).
SAFER K-64	[T.36] L'algorithme de chiffrement sûr et rapide par clé de 64 bits (*secure and fast encryption routine with 64-bit key algorithm*), développé par J. L. Massey en 1993, est un algorithme itératif de chiffrement par blocs qui transforme chaque bloc de texte en clair de 64 bits en un bloc de texte chiffré de 64 bits (voir A. Menezes et al., Handbook of Applied Cryptography, CRC Press, 1997).
SCn	[T.36] Clé d'épreuve secrète, numéro n (*secret challenge key, number n*). Nombre de 12 chiffres décimaux.
SDH	[M.3010] Hiérarchie numérique synchrone (*synchronous digital hierarchy*)
SDP	[J.170] Protocole de description de session (*session description protocol*).
SDU	[H.235] Unité de données de service (*service data unit*)
SG	[J.170] Une passerelle de signalisation (*signalling gateway*) est un agent de signalisation qui reçoit/envoie la signalisation issue du RCS à la frontière du réseau IP. En particulier, la fonction SG du SS7 traduit des variantes de sous-système ISUP ou TCAP de passerelle Internet SS7 en une version commune de sous-système ISUP ou TCAP.

Acronyme	Définition
SH	[T.36] Valeur de hachage embrouillée (*scrambled plain hash*) (24 chiffres décimaux)
SHA-1	[H.235] Algorithme de hachage sécurisé N° 1 (*secure hash algorithm no.1*)
SI	[X.810] Information de sécurité (*security information*)
SIP	[J.170] [X.805] Protocole d'ouverture de session (*session initiation protocol*). Protocole (de signalisation) de commande de la couche application permettant de créer, de modifier et de terminer des sessions avec un ou plusieurs participants.
SIP+	[J.170] Protocole d'ouverture de session plus (*session initiation protocol plus*). Extension de SIP.
SK	[T.36] Clé secrète (*secret key*) pouvant être une clé SCn, SRn, SSn, etc. Nombre de 12 chiffres décimaux.
SMAPM	[X.790] Machine de protocole d'application de gestion-systèmes (*system management application protocol machine*)
SMK	[M.3010] Connaissance de gestion partagée (*shared management knowledge*)
SML	[M.3010] [M.3210.1] Couche de gestion de service (*service management layer*)
SMO	[X.790] Aperçu de la gestion-systèmes (*systems management overview*)
SMTP	[X.805] Protocole de transfert de courrier simple (*simple mail transfer protocol*)
SNMP	[J.170] [X.805] Protocole simple de gestion de réseau (*simple network management protocol*)
SNTP	[H.530] Protocole simple relatif au temps dans le réseau (*simple network time protocol*)
SOA	[X.509] Source d'autorité (*source of authority*)
SONET	[X.805] Réseau optique synchrone (*synchronous optical network*)
S-OSF	[M.3010] Fonction de système d'exploitation – couche de gestion de service (*service management layer – operations systems function*)
SRn	[T.36] Clé de réponse secrète, numéro n (*secret response key, number n*). Nombre de 12 chiffres décimaux.
SRTP	[H.225.0] [H.235] Protocole de transport en temps réel sécurisé (*secure real time protocol*)
SS	[T.36] Clé de session secrète (*secret session key*) utilisée avec l'algorithme d'intégrité HFX40-I (12 chiffres décimaux)
SS7	[J.170] [X.805] Le système de signalisation numéro 7 (*signalling system number 7*) est une architecture et un ensemble de protocoles assurant la signalisation d'appel hors-bande dans un réseau téléphonique.
SSK	[T.36] Clé secrète embrouillée (*scrambled secret key*). Nombre de 12 chiffres décimaux.
SSL	[H.235] [X.805] Couche de connexion sécurisée (*secure socket layer*)
SSn	[T.36] Clé de session secrète, numéro n (*secret session key, number n*), à utiliser avec la fonction de chiffrement ou de hachage. Nombre de 12 chiffres décimaux.
SSx	[T.36] Clé de session secrète créée par X (*secret session key generated by X*) et à utiliser avec l'algorithme de chiffrement HFX40 (12 chiffres décimaux)
TCAP	[J.170] Protocole d'application pour la gestion des transactions (*transaction capabilities application protocol*). Protocole de la pile de protocoles du système SS7 utilisé pour exécuter des transactions entre bases de données distantes avec un point de commande de signalisation.
TD	[J.170] Temporisation de déconnexion (*timeout for disconnect*)
TF	[M.3010] Fonction de transformation (*transformation function*)
TF-MAF	[M.3010] Fonction de transformation – Fonction d'application de gestion (*transformation function – management application function*)
TFTP	[J.170] Protocole trivial de transfert de fichiers (*trivial file transfer protocol*)
TGS	[J.170] Le serveur-distributeur de tickets (*ticket granting server*) est un sous-système du centre KDC utilisé pour distribuer des tickets Kerberos.
TKx	[T.36] Clé de transfert, résultat du chiffrement de la primitive MPx produite par X (*transfer key, an encryption of MPx generated by X*). Nombre de 16 chiffres décimaux.

Acronyme	Définition
TLS	[H.235] Sécurité de la couche transport (*transport level security*)
T_n	[H.530] Horodate numéro n (*timestamp number n*)
TSAP	[H.235] Point d'accès au service de transport (*transport service access point*)
TSP	[X.790] Priorité des services de télécommunication (*telecommunication service priority*)
TTP	[X.810] Tiers de confiance (*trusted third party*)
TTR	[X.790] Dossier de dérangement relatif aux télécommunications (*telecommunications trouble report*)
UCN	[T.36] Nombre crypté unique (*unique crypt number*), par exemple UCNx, UCNy. Nombre de 16 chiffres décimaux connu du système uniquement.
UDP	[J.170] Protocole de datagramme d'utilisateur (*user datagram protocol*).
UIN	[T.36] Numéro d'identité unique (*unique identity number*), par exemple UINx, UINy. Nombre de 48 chiffres décimaux connu du système uniquement.
V-BE	[H.530] Elément frontière du domaine visité (*visited BE*)
V-GK	[H.530] Portier du domaine visité (*visited GK*)
VLF	[H.530] Fonction de localisation dans le domaine visité (*visitor location function*)
VoIP	[X.805] Téléphonie IP, voix sur IP (*voice over IP*)
VPN	[X.805] Réseau privé virtuel (*virtual private network*)
W	[H.530] Valeur composée au moyen d'une combinaison arithmétique de demi-clés de Diffie-Hellman
WSF	[M.3010] Fonction de poste de travail (*workstation function*)
WSSF	[M.3010] Fonction support de poste de travail (*workstation support function*)
WT	[H.530] Jeton ClearToken pour la mobilité (*mobility cleartoken*)
X	[T.36] Nom d'une entité
x	[T.36] Suffixe indiquant qu'un élément appartient à X ou est créé par X
X<<Y>>	[H.234] Certificat de Y émis par X
XOR	[T.36] [H.235] OU exclusif
Xp	[H.234] Clé RSA publique de l'entité X
Xp[*]	[H.234] Chiffrement/déchiffrement de [*] avec Xp. Dans le cas de RSA, on procède par exponentiation.
Xs	[H.234] Clé RSA secrète de l'entité X
Xs[*]	[H.234] Chiffrement/déchiffrement de [*] avec Xs. Dans le cas de RSA, on procède par exponentiation.
XT	[H.530] Jeton CryptoToken pour l'authentification du terminal mobile (*cryptotoken for MT authentication*)
Y	[T.36] Nom d'une deuxième entité
y	[T.36] Suffixe indiquant qu'un élément appartient à Y ou est créé par Y
ZZ	[H.530] Secret partagé/mot de passe de l'utilisateur mobile, partagé avec la fonction AuF correspondante
ZZMT	[H.530] Secret partagé du terminal mobile (MT), partagé avec la fonction AuF correspondante
ZZ_n	[H.530] Secret partagé numéro n (*shared-secret number n*)

A.2 Termes relatifs à la sécurité fréquemment utilisés

Terme	Définition
Contrôle d'accès (*access control*)	[H.235] [X.800] Précaution prise contre l'utilisation non autorisée d'une ressource; cela comprend les précautions prises contre l'utilisation d'une ressource de façon non autorisée (X.800). [J.170] Restriction du flux d'informations provenant des ressources d'un système aux personnes, programmes, processus ou autres ressources de système de réseau autorisés. [X.805] La dimension de sécurité concernant le contrôle d'accès protège contre l'emploi non autorisé des ressources du réseau. Le contrôle d'accès assure que seuls les personnes ou les dispositifs autorisés peuvent accéder aux éléments de réseau, aux flux d'informations, aux services et aux applications. En outre, le contrôle d'accès en fonction du rôle (RBAC, *role-based access control*) institue différents niveaux d'accès, afin de garantir que les personnes et les dispositifs ne peuvent avoir accès aux éléments de réseau, aux informations emmagasinées et aux flux d'informations et ne peuvent les manipuler que s'ils y ont été autorisés.
Liste de contrôle d'accès (*access control list*)	[X.800] Liste des entités qui sont autorisées à accéder à une ressource, avec leurs autorisations d'accès.
Nœud d'accès (*access node*)	[J.170] Dans ce document, un nœud d'accès est un dispositif de terminaison de couche 2 formant l'extrémité réseau de la connexion CM. Dépend de la technique employée. Appelé INA [adaptateur de réseau interactif (*interactive network adapter*)] dans l'Annexe A/J.112 et CMTS [système de terminaison de câblo-modem (*cable modem termination system*)] dans l'Annexe B.
Imputabilité (*accountability*)	[X.800] Propriété qui garantit que les actions d'une entité ne peuvent être imputées qu'à cette entité.
Menace active (*active threat*)	[X.800] Menace de modification non autorisée et délibérée de l'état du système. (Note – La modification et la répétition de messages, l'insertion de faux messages, l'usurpation de l'identité d'une entité autorisée et le déni de service sont des exemples de menaces actives.)
Agent	[X.790] Comme défini dans la Recommandation X.701 – aperçu général concernant la gestion-système (SMO) – mais avec la restriction suivante. Le service devra pouvoir être géré avec un système jouant le rôle de gestionnaire et l'autre jouant le rôle d'agent en ce qui concerne une instance donnée de service ou de ressource de télécommunication.
Alias	[X.790] Nom supplémentaire, en plus de l'identificateur d'objet, sous lequel un dossier de dérangement peut être connu, référencé ou identifié (en général par le client).
Association d'application (*application association*)	[X.790] Relation de coopération entre deux entités d'application, constituée par l'échange d'informations de commande de protocole d'application au moyen de l'utilisation des services de présentation.
Contexte d'application (*application context*)	[X.790] Ensemble d'éléments de service d'application identifié d'une manière explicite, d'options associées et de toute autre information nécessaire à l'interaction d'entités d'application au moyen d'une association d'application.
Entité d'application (*application entity*)	[X.790] Aspects d'un processus d'application se rapportant à l'interconnexion OSI.

Terme	Définition
Alarmes associées (*associated alarms*)	[X.790] Alarmes directement liées à un dérangement identifié explicitement.
Algorithme asymétrique de cryptographie (*asymmetric cryptographic algorithm*)	[X.810] Algorithme pour réaliser le chiffrement ou le déchiffrement correspondant dans lequel les clés utilisées pour le chiffrement et le déchiffrement sont différentes. (NOTE – Avec certains algorithmes asymétriques de cryptographie, il faut utiliser plus d'une clé privée pour déchiffrer un cryptogramme ou pour générer une signature numérique.)
Attaque (*attack*)	[H.235] Activités entreprises pour contourner ou exploiter des déficiences constatées dans les mécanismes de sécurité d'un système. Une attaque directe d'un système exploite des déficiences dans les algorithmes, principes ou propriétés sous-tendant un mécanisme de sécurité. Les attaques indirectes consistent à contourner le mécanisme ou à en provoquer une utilisation incorrecte par le système.
Attribut (*attribute*)	[X.790] Information concernant un objet géré, utilisée pour décrire tout ou partie de cet objet. L'information se constitue d'un type d'attribut et de la valeur d'attribut correspondante qui peut être une valeur simple ou multiple.
Autorité d'attribut (*attribute authority*)	[X.509] Autorité qui attribue des privilèges par l'émission de certificats d'attribut.
Liste de révocation d'autorité d'attribut (*attribute authority revocation list*)	[X.509] Liste de révocation contenant une liste de références de certificats d'attribut concernant des autorités d'attribut qui ne sont plus considérées comme valides par l'autorité émettrice.
Certificat d'attribut (*attribute certificate*)	[X.509] Structure de donnée, portant la signature numérique d'une autorité d'attribut, qui lie certaines valeurs d'attribut à des informations d'identification concernant son détenteur.
Liste de révocation de certificat d'attribut (*attribute certificate revocation list*)	[X.509] Liste de révocation contenant une liste de références de certificats d'attribut qui ne sont plus considérés comme valides par l'autorité émettrice.
Type d'attribut (*attribute type*)	[X.790] Partie d'un attribut indiquant la classe de l'information représentée par cet attribut.
Valeur d'attribut (*attribute value*)	[X.790] Instance particulière de la classe d'information définie par le type d'attribut.
Serveur audio (*audio server*)	[J.170] Un serveur audio passe des annonces d'information dans un réseau IPCablecom. Des annonces de média sont nécessaires pour les communications qui n'aboutissent pas ainsi que pour fournir des services d'information améliorés à l'utilisateur. Les services de serveur audio utilisent des lecteurs de média et des contrôleurs de lecteur de média.
Audit	[X.800] Voir audit de sécurité (*security audit*).
Journal d'audit (*audit trail*)	[X.800] Voir journal d'audit de sécurité(*security audit trail*).

Terme	Définition
Authentification (*authentication*)	[H.235] [X.800] [X.811] Attestation de l'identité revendiquée par une entité. Voir authentification de l'origine des données (*data origin authentication*) et authentification de l'entité homologue (*peer entity authentication*). (Note – Le terme authentification n'est pas associé à l'intégrité des données; le terme intégrité des données est utilisé à la place.) [J.170] Processus consistant à vérifier l'identité déclarée d'une entité auprès d'une autre entité. [X.805] La dimension de sécurité concernant l'authentification sert à confirmer les identités des entités qui communiquent. L'authentification assure la validité des identités déclarées des entités en communication (par exemple, une personne, un dispositif, un service ou une application) et donne l'assurance qu'une entité ne tente pas d'usurper l'identité d'une autre entité ou de reprendre sans autorisation une précédente communication.
Echange d'authentification (*authentication exchange*)	[X.800] Mécanisme destiné à garantir l'identité d'une entité par échange d'informations.
Fonction d'authentification (*authentication function*)	[H.530] Entité fonctionnelle de sécurité qui appartient au domaine de rattachement et qui maintient une relation de sécurité avec les utilisateurs mobiles abonnés et les terminaux mobiles abonnés.
Information d'authentification (*authentication information*)	[X.800] Information utilisée pour établir la validité d'une identité déclarée.
Jeton d'authentification; jeton (*authentication token; token*)	[X.509] Information véhiculée pendant un échange d'authentification forte et pouvant être utilisée pour authentifier son émetteur.
Authenticité (*authenticity*)	[J.170] Capacité de garantir que l'information donnée n'a été ni modifiée ni falsifiée et qu'elle a bien été produite par l'entité qui déclare l'avoir fournie.
Autorité (*authority*)	[X.509] Entité responsable de l'émission de certificats. Cette spécification définit les deux types suivants: les autorités de certification émettant des certificats de clé publique et les autorités d'attribut émettant des certificats d'attribut.
Certificat d'autorité (*authority certificate*)	[X.509] Certificat émis à destination d'une autorité (par exemple, une autorité de certification ou une autorité d'attribut).
Autorisation (*authorization*)	[H.235] Octroi d'une permission sur la base d'une identité authentifiée. [J.170] Fait de donner l'accès à un service ou à un dispositif à quelqu'un qui dispose de la permission d'accès. [X.800] Attribution de droits, comprenant la permission d'accès sur la base de droits d'accès.
Disponibilité (*availability*)	[X.800] Propriété d'être accessible et utilisable sur demande par une entité autorisée.
Disponibilité (*availability*)	[X.805] La dimension de sécurité concernant la disponibilité assure qu'il n'y a pas déni de l'accès autorisé aux éléments de réseau, aux informations emmagasinées, aux flux d'informations, aux services et aux applications en raison d'événements ayant une incidence sur le réseau. Des solutions de récupération en cas de catastrophe sont aussi comprises dans cette catégorie.

Terme	Définition
Liste CRL de base (*base CRL*)	[X.509] Liste CRL utilisée comme base pour la création d'une liste dCRL.
Couche de gestion de l'activité de l'entreprise (*business management layer*)	[M.3010] Couche de gestion responsable de l'intégralité de l'entreprise, et ne faisant pas l'objet d'une normalisation.
Certificat d'autorité de certification (*CA-certificate*)	[X.509] Certificat émis par une autorité de certification pour une autre autorité de certification.
Résilié (*cancelled*)	[X.790] Un gestionnaire peut demander à l'agent de "résilier" un dossier de dérangement, soit parce que ce dernier a été saisi par erreur, soit parce que le dérangement n'existe plus. Dans certaines conditions, par exemple si le dérangement n'a pas encore été affecté ou testé, l'agent "résiliera" le dossier de dérangement en positionnant l'état du dossier sur "liquidé à la demande du client". La résiliation d'un dossier de dérangement peut également avoir des implications commerciales qui sont en dehors du domaine d'application de cette Recommandation, par exemple dans l'éventualité de facturation du dossier de dérangement au client.
Capacité (*capability*)	[X.800] Jeton utilisé comme identificateur d'une ressource de telle sorte que la possession du jeton confère des droits d'accès à cette ressource.
Certificat (*certificate*)	[H.235] Ensemble de données relatives à la sécurité, émis par une autorité de sécurité ou par un tiers de confiance en même temps que des informations de sécurité qui sont utilisées pour fournir les services d'intégrité et d'authentification d'origine des données (Rec. UIT-T X.810). Dans cette Recommandation, ce terme vise des certificats "à clé publique" qui sont des valeurs représentant une clé publique de détenteur (et d'autres informations facultatives), ces valeurs ayant été vérifiées et signées par une autorité de confiance sous une forme infalsifiable.
Politique de certificat (*certificate policy*)	[X.509] Ensemble nommé de règles indiquant la possibilité d'appliquer un certificat pour une communauté particulière et/ou une classe d'applications particulière avec des besoins de sécurité communs. Une politique de certificat particulière peut, par exemple, indiquer la possibilité d'application d'un certificat pour des transactions avec échange de données électroniques pour le commerce de biens dans une fourchette de prix donnée.
Liste de révocation de certificat (*certificate revocation list*)	[X.509] Liste signée indiquant un ensemble de certificats qui ne sont plus considérés comme valides par leur émetteur. Certains types de listes CRL spécifiques sont définis en plus du type générique de liste CRL, pour couvrir des domaines particuliers.
Numéro de série de certificat (*certificate serial number*)	[X.509] Valeur entière, non ambiguë pour l'autorité émettrice, qui est associée de manière biunivoque à un certificat émis par cette autorité de certification.
Utilisateur de certificat (*certificate user*)	[X.509] Entité qui a besoin de connaître avec certitude la clé publique d'une autre entité.
Validation de certificat (*certificate validation*)	[X.509] Processus consistant à s'assurer qu'un certificat était valide à un instant donné, impliquant éventuellement la construction et le traitement d'un itinéraire de certification avec la garantie que tous les certificats de l'itinéraire étaient valides (c'est-à-dire, non caducs ou révoqués) à l'instant donné.

Terme	Définition
Système utilisant des certificats (*certificate-using system*)	[X.509] Implémentation de celles des fonctions définies dans cette Spécification d'annuaire qui sont mises en œuvre par un utilisateur de certificat.
Autorité de certification (*certification authority*)	[X.509] Autorité jouissant de la confiance d'un ou de plusieurs utilisateurs pour la création et l'attribution de certificats. L'autorité de certification peut, de manière optionnelle, créer les clés des utilisateurs. [X.810] Entité habilitée à laquelle il est fait confiance (dans le contexte d'une politique de sécurité) pour créer des certificats de sécurité contenant une ou plusieurs classes de données relatives à la sécurité.
Liste de révocation d'autorité de certification (*certification authority revocation list*)	[X.509] Liste de révocation contenant une liste de certificats de clé publique émise pour des autorités de certification qui ne sont plus considérées comme valides par l'émetteur du certificat.
Itinéraire de certification (*certification path*)	[X.509] Séquence ordonnée de certificats concernant des objets contenus dans l'arbre DIT et qui peuvent être traités à partir de la clé publique de l'objet initial de l'itinéraire pour obtenir l'objet final de cet itinéraire.
Voie (*channel*)	[X.800] Chemin de transfert de l'information.
Chiffre (*cipher*)	[H.235] Algorithme cryptographique ou transformée mathématique. [J.170] Algorithme qui convertit un texte en clair en texte chiffré.
Suite de chiffrement (*ciphersuite*)	[J.170] Ensemble qui doit contenir un algorithme de chiffrement et un algorithme d'authentification de message (par exemple MAC ou HMAC). En général, il peut aussi contenir un algorithme de gestion de clés, qui ne s'applique pas dans le contexte d'IPCablecom.
Cryptogramme, texte chiffré (*ciphertext*)	[X.800] Données obtenues par l'utilisation du chiffrement. Le contenu sémantique des données résultantes n'est pas compréhensible. (Note – Le cryptogramme peut lui-même être réinjecté dans un nouveau chiffrement pour produire un cryptogramme surchiffré.)
Solder des dossiers de dérangement (*clearing trouble reports*)	[X.790] Déclaration faite par un agent indiquant que les actions qui ont été identifiées dans le dossier de dérangement ou que les instances de l'objet activité de réparation ont été exécutées correctement en vue de la résolution du dérangement ou que de telles actions ne sont plus nécessaires. Dans les deux cas le dossier de dérangement devient candidat pour une clôture.
Texte en clair (*cleartext*)	[X.800] Données intelligibles dont la sémantique est compréhensible.
Client	[X.790] Utilisateur d'un service fourni par un système ou un réseau.
Liquidé (*closed-out*)	[X.790] Un dossier de dérangement est considéré comme «liquidé» lorsque le dérangement concerné a été résolu ou n'existe plus et que l'agent met à jour le statut du dossier de dérangement pour indiquer que le dossier de dérangement est «liquidé». Seul l'agent peut faire passer l'état du dossier de dérangement sur «liquidé». Le statut d'un dossier de dérangement peut passer en «liquidé à la demande du client» à la suite d'une demande d'annulation du dossier de dérangement faite par le gestionnaire.
Fermeture des dossiers de dérangement (*closing trouble reports*)	[X.790] Déclaration faite par un agent que le dérangement a été résolu, de sorte que le dossier de dérangement résolu ne pourra plus être traité ultérieurement que pour générer un enregistrement d'historique de dérangement et/ou pour être supprimé.

Terme	Définition
Communication (*communication*)	[X.805] La dimension de sécurité concernant la communication assure que les informations ne seront acheminées qu'entre les extrémités autorisées (les informations ne sont ni déviées ni interceptées au cours de leur acheminement entre ces points).
Entité de confiance conditionnelle (*conditionally trusted entity*)	[X.810] Entité à laquelle il est fait confiance dans le contexte d'une politique de sécurité, mais qui ne peut pas violer la politique de sécurité sans être détectée.
Confidentialité (*confidentiality*)	[H.235] Caractéristique qui empêche la divulgation des informations à des individus, entités ou processus non autorisés. [J.170] Moyen permettant de garantir que les informations ne sont divulguées à personne d'autre qu'aux parties souhaitées. Les informations sont chiffrées pour pouvoir en assurer la confidentialité. On parle aussi de respect de la vie privée. [X.800] Propriété d'une information qui n'est ni disponible, ni divulguée aux personnes, entités ou processus non autorisés.
Entité de gestion conforme (*conformant management entity*)	[X.790] Système ouvert prenant en charge l'interface interopérable définie dans cette Recommandation.
Contact	[X.790] Personne pouvant fournir, au profit du gestionnaire ou de l'agent, une information complémentaire concernant le dérangement.
Pouvoir (*credential*)	[H.530] Dans cette Recommandation, un pouvoir [par exemple $HMAC_{ZZ}(GK_{ID})$ ou $HMAC_{ZZ}(W)$] désigne des données que la fonction AuF a cryptées au moyen du secret *ZZ* qu'elle partage avec l'utilisateur mobile. Le pouvoir est transféré pour prouver que l'autorisation a été accordée et qu'elle a été vérifiée en temps voulu.
Justificatif d'identité (*credentials*)	[X.800] Données transférées pour établir l'identité déclarée d'une entité.
Point de répartition de liste CRL (*CRL distribution point*)	[X.509] Elément de dictionnaire ou autre source de distribution de listes CRL; une telle liste distribuée par le biais d'un point de répartition de liste CRL peut contenir des éléments révoquant uniquement un sous-ensemble de la totalité des certificats émis par une autorité de certification ou peut contenir des éléments révoquant plusieurs autorités de certification.
Analyse cryptographique (*cryptanalysis*)	[J.170] Processus consistant à récupérer le texte en clair d'un message ou la clé de chiffrement sans avoir accès à la clé. [X.800] Analyse d'un système cryptographique, et/ou de ses entrées et sorties, pour en déduire des variables confidentielles et/ou des données sensibles (y compris un texte en clair).
Algorithme cryptographique (*cryptographic algorithm*)	[H.235] Fonction mathématique qui calcule un résultat à partir d'une ou de plusieurs valeurs d'entrée.
Chaînage cryptographique (*cryptographic chaining*)	[X.810] Mode d'utilisation d'un algorithme cryptographique dans lequel la transformation effectuée par l'algorithme dépend des valeurs des entrées ou sorties précédentes.

Terme	Définition
Valeur de contrôle cryptographique (*cryptographic checkvalue*)	[X.800] Information obtenue en réalisant une transformation cryptographique sur une unité de données. (Note – La valeur de contrôle peut être obtenue en une ou plusieurs étapes et résulte d'une fonction mathématique utilisant la clé et une unité de données. Elle permet de vérifier l'intégrité d'une unité de données.)
Système de chiffrement (*cryptographic system, cryptosystem*)	[X.509] Ensemble de transformations d'un texte en clair pour obtenir un texte chiffré et réciproquement, le choix de la ou des transformations particulières à utiliser se faisant au moyen de clés. Les transformations sont définies en général par un algorithme mathématique.
Cryptographie (*cryptography*)	[X.800] Discipline incluant les principes, moyens et méthodes de transformation des données, dans le but de cacher leur contenu, d'empêcher que leur modification passe inaperçue et/ou d'empêcher leur utilisation non autorisée. (Note – La cryptographie détermine les méthodes de chiffrement et de déchiffrement. Une attaque portant sur les principes, moyens et méthodes de cryptographie est appelée analyse cryptographique.)
Client (*customer*)	[X.790] Toute personne qui choisit d'utiliser l'interface OSI OS-OS (entre systèmes d'exploitation) pour effectuer, à travers des domaines de compétence, une gestion de réseau ayant pour objet de gérer des services ou des ressources de télécommunication offerts par un prestataire de services. Le client, ou son représentant, joue le rôle de gestionnaire. Il n'existe pas d'exigence pour que l'interface se limite à un mode de relation entre parties correspondant à un service de téléphonie classique fourni à un client. Il est possible que deux opérateurs puissent utiliser cette interface pour échanger des dossiers de dérangement. Dans un tel cas, le rôle de client peut changer de temps à autre. Une telle relation peut toutefois se décomposer en deux relations gestionnaire-agent.
Réseau de communication de données (*data communication network*)	[M.3010] Réseau de communication à l'intérieur d'un RGT ou entre des RGT qui assurent la fonction de communication de données (DCF).
Confidentialité des données (*data confidentiality*)	[X.509] Ce service peut être utilisé pour protéger des données contre une divulgation non autorisée. Le service de confidentialité des données est pris en charge par le cadre d'authentification. Il peut être utilisé pour protéger des données contre les interceptions. [X.805] La dimension de sécurité concernant la confidentialité des données protège les données contre toute divulgation non autorisée. La confidentialité des données assure que le contenu des données ne pourra être compris par des entités non autorisées. Le chiffrement, les listes de contrôle d'accès et les permissions d'accès aux fichiers sont des méthodes souvent employées pour assurer la confidentialité des données.
Intégrité des données (*data integrity*)	[X.800] Propriété assurant que des données n'ont pas été modifiées ou détruites de façon non autorisée. [X.805] La dimension de sécurité concernant l'intégrité des données assure l'exactitude ou la précision des données. Les données sont protégées contre toute modification, suppression, création et reproduction non autorisées. Cette dimension signale ces activités non autorisées.

Terme	Définition
Authentification de l'origine des données (*data origin authentication*)	[X.800] Confirmation que la source des données reçues est telle que déclarée.
Déchiffrement (*decipherment, decryption*)	[X.800] Opération inverse d'un chiffrement réversible.
Suspendre (*defer*)	[X.790] Retarder le travail concernant un dossier de dérangement ou mettre ce dernier de côté en attendant que des conditions appropriées soient réunies et qu'il puisse progresser de nouveau.
Délégation (*delegation*)	[X.509] Transfert d'un privilège d'une entité détentrice vers une autre entité.
Itinéraire de délégation (*delegation path*)	[X.509] Séquence ordonnée de certificats qui peuvent, conjointement à l'authentification de l'identité du déclarant, être traités pour vérifier l'authenticité d'un privilège de ce déclarant.
Liste CRL delta (liste dCRL) (*delta-CRL*)	[X.509] Liste de révocation partielle contenant uniquement des éléments pour des certificats dont le statut de révocation a été modifié depuis la publication de la liste CRL de base référencée.
Déni de service (*denial of service*)	[X.800] Impossibilité d'accès à des ressources pour des utilisateurs autorisés ou introduction d'un retard pour le traitement d'opérations critiques.
Empreinte numérique (*digital fingerprint*)	[X.810] Caractéristique d'un élément de données, telle qu'une valeur de contrôle cryptographique ou le résultat de la réalisation d'une fonction de hachage unidirectionnelle sur les données, qui est suffisamment spécifique à l'élément de données pour qu'il ne soit pas possible de trouver, de façon informatique, un autre élément de données ayant les mêmes caractéristiques.
Signature numérique (*digital signature*)	[X.800] Données ajoutées à une unité de données, ou transformation cryptographique d'une unité de données, permettant à un destinataire de prouver la source et l'intégrité de l'unité de données et protégeant contre la falsification (par le destinataire, par exemple).
Identificateur caractéristique (*distinguishing identifier*)	[X.810] Données qui identifient de façon univoque une entité.
Sens aval, sens descendant (*downstream*)	[J.170] Sens allant de la tête de réseau à l'emplacement de l'abonné.
Couche de gestion des éléments (*element management layer*)	[M.3010] Couche de gestion qui est responsable de la gestion des éléments du réseau, soit individuellement, soit collectivement.
Chiffrement (*encipherment, encryption*)	[H.235] Processus consistant à rendre des données illisibles par des entités non autorisées après application d'un algorithme cryptographique (ou de chiffrement). Le déchiffrement est l'opération inverse par laquelle le texte chiffré est transformé en texte clair. [X.800] Transformation cryptographique de données produisant un cryptogramme. (Note – Le chiffrement peut être irréversible. Dans ce cas, le déchiffrement correspondant ne peut pas être effectué.)
Chiffrement (*encryption*)	[J.170] Méthode utilisée pour convertir des informations en clair en cryptogramme. [X.800] Voir chiffrement (*encipherment*).

Terme	Définition
Entité finale (*end entity*)	[X.509] Sujet d'un certificat qui utilise sa clé privée à d'autres fins que la signature de certificats ou entité qui est un participant faisant confiance.
Liste de révocation de certificat d'attribut d'entité finale (*end-entity attribute certificate revocation list*)	[X.509] Liste de révocation contenant une liste de certificats d'attribut émis à destination de détenteurs, qui ne sont pas également des autorités d'attribut et qui ne sont plus considérés comme valides par l'émetteur du certificat.
Liste de révocation de certificat de clé publique (*end-entity public-key certificate revocation list*)	[X.509] Liste de révocation contenant une liste de certificats de clé publique, émise à destination de sujets qui ne sont pas également des autorités de certification, et qui ne sont plus considérés comme valides par l'émetteur du certificat.
Point d'extrémité (*endpoint*)	[J.170] Terminal, passerelle ou pont de conférence (MCU).
Chiffrement de bout en bout (*end-to-end encipherment*)	[X.800] Chiffrement de données à l'intérieur ou au niveau du système d'extrémité source, le déchiffrement correspondant ne se produisant qu'à l'intérieur, ou au niveau du système d'extrémité de destination (voir aussi chiffrement liaison par liaison (*link-by-link encipherment*)).
Variables d'environnement (*environmental variables*)	[X.509] Caractéristiques d'une politique nécessaires pour une décision d'autorisation, qui ne sont pas contenues dans des structures statiques mais qui sont accessibles localement par un vérificateur de privilège (par exemple, le jour et l'heure ou le solde actuel d'un compte).
Escalade d'un dossier de dérangement (*escalating a trouble report*)	[X.790] Identification d'un dossier de dérangement devant être pris en considération d'une manière urgente et immédiate par une autorité supérieure en vue de la résolution du dérangement.
Evénement (*event*)	[X.790] Une occurrence temporelle qui modifie le statut global d'un objet. La modification du statut peut être persistante ou temporaire, ce qui permet de réaliser des fonctions telles que la surveillance, la supervision ou la mesure des performances. Les événements peuvent générer ou non des comptes rendus, ils peuvent être inopinés ou planifiés, ils peuvent déclencher d'autres événements ou peuvent être déclenchés par un ou plusieurs autres événements.
Message d'événement (*event message*)	[J.170] Message se rapportant à une seule portion de connexion.
Interface f (*F interface*)	[M.3010] Interface appliquée à des points de référence f.
Point de référence f (*f reference point*)	[M.3010] Point de référence situé entre le bloc de fonctions de poste de travail (WSF) et le bloc de fonctions de système d'exploitation (OSF).
Gestion des fautes (*fault management*)	[X.790] La gestion des fautes est constituée d'un ensemble de fonctions permettant la détection, l'isolation et la correction d'un fonctionnement anormal du réseau de télécommunication et de son environnement.
Liste CRL complète (*full CRL*)	[X.509] Liste de révocation complète contenant des éléments pour tous les certificats qui ont été révoqués pour le domaine d'application donné.
Bloc de fonctions (*function block*)	[M.3010] Plus petite unité (pouvant être mise en œuvre) de la fonctionnalité de gestion du RGT faisant l'objet d'une normalisation.

Terme	Définition
Point de référence g (*g reference point*)	[M.3010] Point de référence situé à l'extérieur du RGT entre les utilisateurs (hommes) et le bloc de fonctions de poste de travail (WSF). N'est pas considéré comme faisant partie du RGT même s'il permet l'acheminement de ses informations.
Passerelle (*gateway*)	[J.170] Dispositif servant de pont entre le monde des communications vocales IPCablecom et le RTPC. Il s'agit par exemple de la passerelle média, qui fournit les interfaces de circuit support avec le RTPC et transcode le flux de média, et de la passerelle de signalisation, qui envoie et reçoit la signalisation du réseau à commutation de circuit à la frontière du réseau IPCablecom.
Fonction de hachage (*hash function*)	[X.509] Fonction (mathématique) qui fait correspondre un argument pris dans un domaine étendu (éventuellement très étendu) à une valeur appartenant à un domaine plus réduit. Une "bonne" fonction de hachage est telle que l'application de la fonction à un ensemble (étendu) d'arguments du premier domaine fournira des valeurs réparties de manière égale (apparemment aléatoire) dans le second domaine. [X.810] Fonction (mathématique) qui fait correspondre les valeurs d'un grand ensemble (potentiellement très grand) de valeurs à une gamme plus réduite de valeurs.
En-tête (*header*)	[J.170] Informations de commande de protocole se trouvant au début d'une unité de données de protocole.
Détenteur (*holder*)	[X.509] Entité qui a reçu la délégation d'un privilège, soit directement de la source d'autorité, soit indirectement par le biais d'une autre autorité d'attribut.
Elément frontière du domaine de rattachement (*home border element*)	[H.530] Elément frontière (BE) situé dans le domaine de rattachement.
Politique de sécurité fondée sur l'identité (*identity-based security policy*)	[X.800] Politique de sécurité fondée sur les identités et/ou les attributs des utilisateurs, d'un groupe d'utilisateurs ou d'entités agissant au nom d'utilisateurs et sur les identités et/ou attributs des ressources/objets auxquels on doit accéder.
Liste CRL indirecte (iCRL) (*indirect CRL*)	[X.509] Liste de révocation qui contient au moins une information de révocation concernant des certificats émis par des autorités autres que l'émetteur de cette liste.
Intégrité (*integrity*)	[H.235] Caractéristique de données qui n'ont pas été altérées de façon non autorisée. [J.170] Moyen permettant de garantir que les informations ne sont pas modifiées sauf par ceux qui sont autorisés à le faire. [X.800] Voir intégrité des données (*data integrity*).
Interface	[M.3010] Concept architectural qui assure l'interconnexion de blocs physiques à des points de référence.
Domaine de compétence (*jurisdiction*)	[X.790] Concept se référant à une classification fonctionnelle des réseaux de télécommunication. Un domaine de compétence appartient à l'un des quatre types suivants: a) réseau d'opérateur de centre de commutation local; b) réseau d'opérateur de transit; c) réseau de client final; d) une combinaison des précédents.
Kerberos	[J.170] Protocole d'authentification de réseau à clé secrète qui utilise plusieurs algorithmes cryptographiques pour le chiffrement et une base de données de clés centralisée pour l'authentification.

Terme	Définition
Clé (*key*)	[J.170] Valeur mathématique introduite dans l'algorithme cryptographique choisi. [X.800] Série de symboles commandant les opérations de chiffrement et de déchiffrement.
Agrément de clé (*key agreement*)	[X.509] Méthode de négociation en ligne de la valeur d'une clé sans transfert de cette dernière, même sous forme chiffrée, par exemple en utilisant la méthode Diffie-Hellman (se référer à ISO/CEI 11770-1 pour plus d'informations concernant les procédés d'agrément de clé).
Echange de clés (*key exchange*)	[J.170] Echange de clés publiques entre entités à utiliser pour le chiffrement des communications entre ces entités.
Gestion de clés (*key management*)	[H.235] [X.800] Production, stockage, distribution, suppression, archivage et application de clés conformément à une politique de sécurité.
Gestion de clés (*key-management*)	[J.170] Distribution des clés symétriques partagées nécessaires à l'exécution d'un protocole de sécurité.
Chiffrement liaison par liaison (*link-by-link encipherment*)	[X.800] Application particulière du chiffrement à chaque liaison d'un système de communication (voir aussi chiffrement de bout en bout (*end-to-end encipherment*)). (Note – Le chiffrement liaison par liaison implique que les données soient du texte en clair dans les entités relais.)
Architecture logique répartie en couches (*logical layered architecture*)	[M.3010] Concept architectural qui organise les fonctions de gestion sous forme d'un groupement des couches de gestion et qui décrit la relation existant entre les couches.
Point de référence m (*m reference point*)	[M.3010] Point de référence situé à l'extérieur du RGT entre un bloc de fonctions d'adaptateur Q (QAF) et des entités gérées non conformes aux Recommandations relatives au RGT.
Ressource gérée (*managed resource*)	[M.3010] Abstraction des aspects d'une ressource (logique ou physique) de télécommunication nécessaire à la gestion des télécommunications.
Fonction d'application de gestion (*management application function*)	[M.3010] Fonction qui représente (une partie de) la fonctionnalité d'un seul ou de plusieurs services de gestion.
Domaine de gestion (*management domain*)	[M.3010] Ensemble de ressources gérées faisant l'objet d'une politique de gestion commune.
Fonction de gestion (*management function*)	[M.3010] Plus petite partie d'un service de gestion qui est perçue par l'utilisateur du service.
Ensemble de fonctions de gestion (*management function set*)	[M.3010] Groupement de fonctions de gestion RGT appartenant à un même contexte, c'est-à-dire se rapportant à une capacité de gestion donnée (fonctions de signalisation d'alarme, commande de gestion de trafic, par exemple). L'ensemble de fonctions de gestion RGT est le plus petit élément réutilisable de la spécification fonctionnelle. Il doit être considéré comme un tout. Il est analogue à la partie besoins de la fonction de gestion des systèmes OSI (OSI SMF).
Service de gestion (*management service*)	[M.3010] Service satisfaisant des besoins spécifiques de gestion des télécommunications.
Couche de gestion (*management layer*)	[M.3010] Concept architectural qui reflète des aspects particuliers de la gestion et qui suppose un regroupement des informations de gestion correspondant à ces aspects.

Terme	Définition
Gestionnaire (*manager*)	[X.790] Comme défini dans la Recommandation X.701 – Aperçu général de la gestion-système (SMO), mais avec la restriction suivante. Le service devra pouvoir être géré avec un système jouant le rôle de gestionnaire et l'autre jouant le rôle d'agent en ce qui concerne une instance donnée de service ou de ressource de télécommunication.
Détection de modification (*manipulation detection*)	[X.800] Mécanisme utilisé pour détecter les modifications, accidentelles ou intentionnelles, d'une unité de données.
Usurpation d'identité (*masquerade*)	[X.800] Prétention qu'a une entité d'en être une autre.
Flux média (*media stream*)	[H.235] Flux audio, vidéo ou de données, ou combinaison quelconque de ces types de flux. Les flux médias acheminent des données d'utilisateur ou d'application (charge utile) mais pas de données de commande.
Proxy de routage pour la mobilité (*mobility routing proxy*)	[H.530] Entité fonctionnelle facultative qui joue le rôle d'une entité fonctionnelle intermédiaire, terminant l'association de sécurité d'une liaison bond par bond.
Elément de réseau (*network element*)	[M.3010] Concept architectural qui représente un équipement (ou des groupes/parties d'équipement) de télécommunication ainsi que l'équipement d'appui, ou toute entité ou tout groupe d'entités considérés comme appartenant à l'environnement de télécommunication qui exerce les fonctions d'élément de réseau (NEF).
Fonction d'élément de réseau (*network element function*)	[M.3010] Bloc de fonctions qui représente les fonctions de télécommunication et qui communique avec le bloc OSF du RGT afin d'être contrôlé et/ou commandé.
Couche de gestion de réseau (*network management layer*)	[M.3010] Couche de gestion responsable de la gestion d'une vue de réseau et de la coordination de l'activité.
Non-répudiation (*non-repudiation*)	[H.235] Protection contre le déni, par une des entités impliquées dans une communication, d'avoir participé à tout ou partie de celle-ci. [J.170] Capacité d'empêcher à un émetteur de nier ultérieurement avoir envoyé un message ou exécuté une action. [X.805] La dimension de sécurité concernant la non-répudiation donne les moyens d'empêcher une personne ou une entité de nier avoir exécuté une action particulière liée aux données, en fournissant une attestation des diverses actions dans le réseau (telle qu'une attestation d'obligation, d'intention ou d'engagement; une attestation de l'origine des données, une attestation de propriété ou une attestation de l'emploi des ressources). Elle assure la mise à disposition de la preuve qui peut être présentée à une entité tierce et être utilisée pour prouver qu'un certain type d'événement ou d'action a eu lieu.
Notarisation (*notarization*)	[X.800] Enregistrement de données chez un tiers de confiance permettant de s'assurer ultérieurement de leur exactitude (contenu, origine, date, remise).
Méthode d'objet (*object method*)	[X.509] Action pouvant être invoquée pour une ressource (par exemple, un système de fichier peut disposer de méthodes objet de lecture, d'écriture et d'exécution).

Terme	Définition
Fonction unidirectionnelle, fonction non réversible (*one-way function*)	[X.509] Fonction mathématique facile à calculer, mais qui, pour une valeur quelconque y du domaine image, il est difficile de trouver une valeur x du domaine source telle que f(x) = y. Il peut exister un nombre réduit de valeurs de y pour lesquelles le calcul de x est trivial. [X.810] Fonction (mathématique) qu'il est facile de calculer mais pour laquelle, lorsque le résultat est connu, il n'est pas possible de trouver, de façon informatique, n'importe laquelle des valeurs qui auraient pu être fournies pour obtenir celui-ci.
Fonction de hachage unidirectionnelle (*one-way hash function*)	[X.810] Fonction (mathématique) qui est à la fois une fonction unidirectionnelle et une fonction de hachage.
Système d'exploitation (*operations system*)	[M.3010] Bloc physique qui exécute les fonctions du système d'exploitation (OSF).
Fonction des systèmes d'exploitation (*operations systems function*)	[M.3010] Bloc de fonctions qui traite les informations relatives à la gestion des télécommunications afin de contrôler/coordonner et/ou commander les fonctions de télécommunication, parmi lesquelles les fonctions de gestion (c'est-à-dire le RGT lui-même).
Interruption de service (*outage*)	[X.790] Indisponibilité d'un service ou d'une ressource.
Menace passive (*passive threat*)	[X.800] Menace d'une divulgation non autorisée des informations, sans que l'état du système ne soit modifié.
Mot de passe (*password*)	[H.530] [X.800] Information d'authentification confidentielle, habituellement composée d'une chaîne de caractères.
Authentification de l'entité homologue (*peer-entity authentication*)	[X.800] Confirmation qu'une entité homologue d'une association est bien l'entité déclarée.
Gravité perçue (*perceived severity*)	[X.790] Gravité du problème telle qu'elle est perçue par la personne qui signale le dérangement.
Bloc physique (*physical block*)	[M.3010] Concept architectural représentant une réalisation d'un seul ou de plusieurs blocs de fonctions.
Sécurité physique (*physical security*)	[X.800] Mesures prises pour assurer la protection des ressources contre des menaces délibérées ou accidentelles.
Politique (*policy*)	[X.800] Voir politique de sécurité (*security policy*).
Mappage de politique (*policy mapping*)	[X.509] Reconnaissance du fait que, lorsqu'une autorité de certification d'un domaine certifie une autorité de certification d'un autre domaine, une politique de certificat propre au deuxième domaine peut être considérée par l'autorité du premier domaine comme équivalente (mais pas nécessairement comme identique sous tous ses aspects) à une politique de certificat dans le premier domaine.
Priorité (*priority*)	[X.790] Degré d'urgence exigé par le gestionnaire pour la résolution du problème.

Terme	Définition
Respect de la vie privée, secret des communications (*privacy*)	[H.235] Mode de communication dans lequel seules les parties explicitement habilitées peuvent interpréter la communication. Le secret des communications est normalement réalisé par chiffrement et par partage de clé(s) pour accéder au chiffre. [J.170] Moyen permettant de garantir que les informations ne sont divulguées à personne d'autre qu'aux parties souhaitées. Les informations sont généralement chiffrées pour pouvoir en assurer la confidentialité. On parle aussi de confidentialité. [X.800] Droit des individus de contrôler ou d'agir sur des informations les concernant, qui peuvent être collectées et stockées, et sur les personnes par lesquelles et auxquelles ces informations peuvent être divulguées. (Note – Ce terme étant lié au droit privé, il ne peut pas être très précis et son utilisation devrait être évitée sauf pour des besoins de sécurité). [X.805] La dimension de sécurité concernant le respect de la vie privée assure la protection des informations qui pourraient être déduites de l'examen des activités dans le réseau. Des exemples de telles informations sont notamment les sites web que l'utilisateur a visités, le lieu géographique de l'utilisateur, ainsi que les adresses IP et les noms DNS de dispositifs dans un réseau de fournisseur de services.
Canal privé (*private channel*)	[H.235] Dans cette Recommandation, un canal privé est celui qui résulte d'une négociation préalable par canal sécurisé et qui peut servir à acheminer des flux médias.
Clé privée (*private key*)	[J.170] Clé utilisée en cryptographie à clé publique qui appartient à une entité individuelle et qui doit être tenue secrète. [X.810] Clé qui est utilisée avec un algorithme asymétrique de cryptographie et dont la possession est limitée (habituellement à une seule entité).
Clé privée; clé secrète (déconseillé) (*private key; secret key*)	[X.509] (Dans un système de chiffrement avec clé publique) celle des clés d'une paire de clés d'un utilisateur qui est connue uniquement par l'utilisateur concerné.
Privilège (*privilege*)	[X.509] Attribut ou propriété attribué par une autorité à un utilisateur.
Déclarant de privilège (*privilege asserter*)	[X.509] Détenteur de privilège utilisant son certificat d'attribut ou de clé publique pour déclarer un privilège.
Infrastructure de gestion de privilège (PMI, *privilege management infrastructure*)	[X.509] Infrastructure qui peut prendre en charge la gestion des privilèges correspondant à un service complet d'autorisation et en relation avec une infrastructure de clé publique.
Politique de privilège (*privilege policy*)	[X.509] Politique qui définit dans ses grandes lignes les conditions sous lesquelles les vérificateurs de privilège peuvent fournir ou effectuer des services sensibles au profit ou pour le compte de déclarants de privilège qualifiés. La politique de privilège est liée à des attributs associés au service, ainsi qu'à des attributs associés aux déclarants de privilège.
Vérificateur de privilège (*privilege verifier*)	[X.509] Entité effectuant la vérification de certificats conformément à une politique de privilège.
Proxy	[J.170] Fonctionnalité qui assure un service de manière indirecte ou qui fournit des informations en tant que représentant, ce qui permet d'éviter à un serveur de devoir prendre en charge le service.

Terme	Définition
Clé publique (*public key*)	[J.170] Clé utilisée en cryptographie à clé publique qui appartient à une entité individuelle et est distribuée publiquement. Les autres entités utilisent cette clé pour chiffrer les données à envoyer au propriétaire de la clé. [X.810] Clé qui est utilisée avec un algorithme asymétrique de cryptographie et qui peut être rendue publique.
Certificat de clé publique (*public key certificate*)	[J.170] Relation entre la clé publique d'une entité et un ou plusieurs attributs relatifs à son identité, également appelé certificat numérique.
Cryptographie à clés publiques (*public key cryptography*)	[H.235] Système de chiffrement qui fait appel (pour le chiffrement et le déchiffrement) à des clés asymétriques liées par une relation mathématique qui ne peut logiquement pas être calculée. [J.170] Procédure qui utilise une paire de clés, une clé publique et une clé privée, pour le chiffrement et le déchiffrement, également appelée algorithme asymétrique. La clé publique d'un utilisateur est rendue publique de sorte que les autres utilisateurs puissent l'utiliser pour envoyer un message au propriétaire de la clé. La clé privée d'un utilisateur est tenue secrète et c'est la seule clé qui permette de déchiffrer les messages envoyés qui ont été chiffrés par la clé publique de l'utilisateur.
Infrastructure de clé publique (PKI, *public key infrastructure*)	[X.509] Infrastructure pouvant prendre en charge la gestion de clés publiques afin de fournir des services d'authentification, de chiffrement, d'intégrité et de non-répudiation.
Exploitant de télécommunications publiques (PTO, *public telecommunication operator*)	[M.3010] Utilisée dans un souci de concision, l'expression couvre les administrations de télécommunication, les exploitations reconnues, les administrations (clients et tiers) et/ou d'autres organisations qui exploitent ou utilisent un réseau de gestion des télécommunications (RGT).
Clé publique (*public-key*)	[X.509] (Dans un système de chiffrement avec clé publique) celle des clés d'une paire de clés d'un utilisateur qui est connue de manière publique.
Certificat de clé publique (*public-key certificate*)	[X.509] Clé publique d'un utilisateur, associée à certaines autres informations qui sont rendues non falsifiables par chiffrement en utilisant la clé privée de l'autorité de certification émettrice.
Adaptateur Q (*Q adapter*)	[M.3010] Bloc physique qui est caractérisé par un bloc de fonctions d'adaptateur Q autonome et qui relie des entités physiques de type NE ou OS dotées d'interfaces non compatibles RGT (au point de référence m) à des interface Q.
Interface Q (*Q interface*)	[M.3010] Interface appliquée aux points de référence q.
Point de référence q (*q reference point*)	[M.3010] Point de référence situé entre les fonctions NEF et OSF, et OSF et OSF.
Point de référence (*reference point*)	[M.3010] Concept architectural utilisé pour délimiter les blocs de fonctions de gestion et qui détermine une frontière de service entre deux blocs de fonctions de gestion.
Participant faisant confiance (*relying party*)	[X.509] Utilisateur ou agent qui fait confiance aux données contenues dans un certificat pour prendre des décisions.
Répudiation (*repudiation*)	[X.800] Le fait, pour une des entités impliquées dans la communication, de nier avoir participé aux échanges, totalement ou en partie.

Terme	Définition
Certificat de révocation (*revocation certificate*)	[X.810] Certificat de sécurité émis par une autorité de sécurité pour indiquer qu'un certificat de sécurité particulier a été révoqué.
Certificat de révocation de liste (*revocation list certificate*)	[X.810] Certificat de sécurité qui identifie une liste de certificats de sécurité qui ont été révoqués.
Certificat d'attribution de rôle (*role assignment certificate*)	[X.509] Certificat contenant l'attribut de rôle qui assigne un ou plusieurs rôles au sujet/au détenteur du certificat.
Certificat de spécification de rôle (*role specification certificate*)	[X.509] Certificat contenant l'attribution de privilèges à un rôle.
Clé privée racine (*root private key*)	[J.170] Clé privée de signature appartenant à l'autorité de certification du niveau le plus élevé. Elle est normalement utilisée pour signer des certificats de clé publique pour les autorités de certification de niveau inférieur ou pour d'autres entités.
Contrôle de routage (*routing control*)	[X.800] Application de règles, au cours du processus de routage, afin de choisir ou d'éviter, des réseaux, liaisons ou relais spécifiques.
Politique de sécurité fondée sur des règles (*rule-based security policy*)	[X.800] Politique de sécurité fondée sur des règles globales imposées à tous les utilisateurs. Ces règles s'appuient généralement sur une comparaison de la sensibilité des ressources auxquelles on doit accéder avec les attributs correspondants d'utilisateurs, d'un groupe d'utilisateurs ou d'entités agissant au nom d'utilisateurs.
Scellé (*seal*)	[X.810] Valeur de contrôle cryptographique qui met en œuvre l'intégrité mais qui ne protège pas d'une falsification du récepteur (c'est-à-dire qu'il n'offre pas la non-répudiation). Lorsqu'un scellé est associé à un élément de données, cet élément de données est dit *scellé*. (Note – Bien qu'un scellé n'offre pas lui-même la non-répudiation, certains mécanismes de non-répudiation font usage du service d'intégrité offert par les scellés, par exemple, pour protéger les communications avec des tierces parties de confiance).
Clé secrète (*secret key*)	[X.810] Clé qui est utilisée avec un algorithme symétrique de cryptographie. La possession de cette clé est limitée (habituellement à deux entités).
Règles d'interaction sécurisée (*secure interaction rules*)	[X.810] Règles de politique de sécurité qui régissent des interactions entre domaines de sécurité.
Administrateur de sécurité (*security administrator*)	[X.810] Personne qui est responsable de la définition ou de l'application d'une ou de plusieurs parties de la politique de sécurité.
Audit de sécurité (*security audit*)	[X.800] Revue indépendante et examen des enregistrements et des activités du système afin de vérifier l'exactitude des contrôles du système pour s'assurer de leur concordance avec la politique de sécurité établie et les procédures d'exploitation, pour détecter les infractions à la sécurité et pour recommander les modifications appropriées des contrôles, de la politique et des procédures.

Terme	Définition
Journal d'audit de sécurité (*security audit trail*)	[X.800] Données collectées et pouvant éventuellement être utilisées pour permettre un audit de sécurité.
Autorité de sécurité (*security authority*)	[X.810] Entité qui est responsable de la définition, de la mise en œuvre ou de l'application de la politique de sécurité.
Certificat de sécurité (*security certificate*)	[X.810] Ensemble de données relatives à la sécurité émis par une autorité de sécurité ou une tierce partie de confiance ainsi que les informations de sécurité qui sont utilisées pour fournir des services d'intégrité et d'authentification de l'origine des données. (Note – Tous les certificats sont réputés être des certificats de sécurité (voir les définitions applicables dans l'ISO 7498-2). Le terme *certificat de sécurité* est adopté afin d'éviter des conflits de terminologie avec la Rec. UIT-T X.509 | ISO/CEI 9594-8 (c'est-à-dire la norme d'authentification de l'annuaire).
Chaîne de certificat de sécurité (*security certificate chain*)	[X.810] Séquence ordonnée de certificats de sécurité, dans laquelle le premier certificat de sécurité contient des informations relatives à la sécurité et les certificats de sécurité suivants contiennent des informations de sécurité qui peuvent être utilisées pour la vérification des certificats de sécurité précédents.
Domaine de sécurité (*security domain*)	[X.810] Ensemble d'éléments, politique de sécurité, autorité de sécurité et ensemble d'activités liées à la sécurité dans lesquels l'ensemble des éléments est sujet à la politique de sécurité, pour les activités spécifiées et la politique de sécurité est administrée par l'autorité de sécurité, pour le domaine de sécurité.
Autorité du domaine de sécurité (*security domain authority*)	[X.810] Autorité de sécurité qui est responsable de la mise en œuvre d'une politique de sécurité pour un domaine de sécurité.
Information de sécurité (*security information*)	[X.810] Information nécessaire pour mettre en œuvre des services de sécurité.
Etiquette de sécurité (*security label*)	[X.800] Marque liée à une ressource dénommant ou désignant les attributs de sécurité de cette ressource (cette ressource peut être une unité de données). (Note – La marque et/ou l'association de la marque à la ressource peuvent être implicites ou explicites.)
Politique de sécurité (*security policy*)	[X.509] Ensemble de règles fixées par l'autorité de sécurité qui régit l'utilisation et la fourniture de services et de fonctionnalités de sécurité. [X.800] Ensemble des critères permettant de fournir des services de sécurité [voir aussi politique de sécurité fondée sur l'identité (*identity-based security policy*) et politique de sécurité fondée sur des règles (*rule-based security policy*)]. (Note – Une politique de sécurité complète traite nécessairement de sujets qui ne relèvent pas du champ d'application de l'OSI.)
Règles de politique de sécurité (*security policy rules*)	[X.810] Représentation d'une politique de sécurité pour un domaine de sécurité au sein d'un système réel.
Profil de sécurité (*security profile*)	[H.235] (Sous-) Ensemble cohérent de procédures et caractéristiques interopérables, tirées de la Rec. UIT-T H.235, très utiles pour sécuriser des communications multimédias H.323 entre des entités concernées dans un scénario donné.

Terme	Définition
Rétablissement de la sécurité (*security recovery*)	[X.810] Actions qui sont menées et procédures qui sont utilisées lorsqu'une violation de sécurité est soit détectée soit soupçonnée d'avoir eu lieu.
Service de sécurité (*security service*)	[X.800] Service, fourni par une couche de systèmes ouverts, garantissant une sécurité des systèmes et du transfert de données.
Jeton de sécurité (*security token*)	[X.810] Ensemble de données protégé par un ou plusieurs services de sécurité, ainsi que les informations de sécurité utilisées pour la fourniture de ces services de sécurité, qui est transféré entre les entités communicantes.
Protection sélective des champs (*selective field protection*)	[X.800] Protection de certains champs spécifiques dans un message à transmettre.
Sensibilité (*sensitivity*)	[X.509] Caractéristique d'une ressource liée à sa valeur ou à son importance. [X.800] Caractéristique d'une ressource relative à sa valeur ou à son importance et, éventuellement, à sa vulnérabilité.
Service (*service*)	[X.790] Terme désignant les capacités qu'un client achète ou loue à un prestataire de services. Un service est une abstraction de la vue basée sur les éléments de réseau ou de la vue basée sur les équipements. Des services identiques peuvent être fournis par différents éléments de réseau et des services différents peuvent être fournis par les mêmes éléments de réseau.
Couche de gestion de service (*service management layer*)	[M.3010] Couche de gestion qui concerne et a en charge les aspects contractuels (traitement des ordres de service, des plaintes et facturation ...) des services qui sont fournis aux clients ou mis à la disposition d'éventuels nouveaux clients.
Fournisseur de service (*service provider*)	[X.790] Système ou réseau fournissant un service de télécommunication à un client. Dans le contexte du présent document, le fournisseur de service est plus spécifiquement un fournisseur de services de télécommunication qui propose une interface OSI entre systèmes ouverts, afin de conférer au client une capacité de gestion de réseau à travers de multiples juridictions, et de lui permettre ainsi de contrôler les services (ou ressources) fournis (voir client (*customex*)). Un fournisseur de service agit dans le rôle d'agent. Il n'existe pas d'exigence pour que l'interface se limite au cas d'une relation classique de client de service de télécommunication à prestataire de service de télécommunication. Il est parfaitement possible que cette interface soit utile à deux transporteurs de télécommunication dont les réseaux interagissent pour fournir un service à un utilisateur final. Dans un tel cas, les rôles de client et de prestataire de service peuvent s'intervertir de temps à autre. Toutefois, dans une situation donnée, un transporteur sera le client et assumera le rôle de gestionnaire, tandis que l'autre sera le fournisseur et assumera le rôle d'agent.
Relation de service (*service relationship*)	[H.530] Association de sécurité établie entre deux entités fonctionnelles pour laquelle au moins une clé partagée est présente.
Secret partagé (*shared secret*)	[H.530] Clé de sécurité pour les algorithmes cryptographiques; le secret partagé peut être déduit d'un mot de passe.
Signature (*signature*)	[X.800] Voir signature numérique (*digital signature*).
Authentification simple (*simple authentication*)	[X.509] Authentification utilisant de simples accords de mot de passe.

Terme	Définition
Source d'autorité (*source of authority*)	[X.509] Autorité d'attribut auquel peut faire confiance un vérificateur de privilège pour une ressource donnée, en tant qu'autorité ultime pour l'attribution d'un ensemble de privilèges.
Submersion (*spamming*)	[H.235] Agression visant à amener un système à une situation de refus de service par l'envoi, à celui-ci, d'un grand nombre de données non autorisées. Un cas particulier est la submersion d'un média par l'envoi de paquets RTP à des ports UDP. Généralement, le système est submergé de paquets et le traitement correspondant nécessite de précieuses ressources
Etat d'un dossier de dérangement (*status of a trouble report*)	[X.790] Etape qui a été atteinte par un dossier de dérangement, au cours de la résolution du dérangement, depuis l'instant de sa création par instanciation.
Authentification forte (*strong authentication*)	[X.509] Authentification utilisant des justificatifs obtenus par des moyens de chiffrement.
Algorithme cryptographique symétrique (à clés secrètes) (*symmetric (secret-key based) cryptographic algorithm*)	[H.235] Algorithme permettant de réaliser le chiffrement ou le déchiffrement correspondant, dans lequel la même clé est requise à la fois pour le chiffrement et pour le déchiffrement (Rec. UIT-T X.810).
Algorithme symétrique de cryptographie (*symmetric cryptographic algorithm*)	[X.810] Algorithme pour réaliser le chiffrement ou algorithme pour réaliser le déchiffrement correspondant dans lequel la même clé est requise à la fois pour le chiffrement et le déchiffrement.
Réseau de gestion des télécommunications (*telecommunications management network*)	[M.3010] Architecture destinée à la gestion (comprenant la planification, la fourniture, l'installation, la maintenance, l'exploitation et l'administration) d'équipements de réseau et de services de télécommunication.
Menace (*threat*)	[H.235] Violation potentielle de la sécurité (Rec. UIT-T X.800). [X.800] Violation potentielle de la sécurité.
Horodatage (*time-stamp*)	[X.790] Valeur de la date et de l'heure indiquant l'instant d'exécution d'une activité ou d'une action ou encore l'instant d'apparition d'un événement.
Analyse du trafic (*traffic analysis*)	[X.800] Déduction d'informations à partir de l'observation des flux de données (présence, absence, quantité, direction, fréquence).
Confidentialité du flux de données (*traffic flow confidentiality*)	[X.800] Service de confidentialité fournissant une protection contre l'analyse du trafic.
Bourrage (*traffic padding*)	[X.800] Production d'instances de communication parasites, d'unités de données parasites et/ou de données parasites dans des unités de données.
Fonction de transformation (*transformation function*)	[M.3010] Bloc de fonctions qui traduit entre un point de référence RGT et un point de référence (soit "propriétaire", soit normalisé) non RGT. La partie non RGT de ce bloc de fonctions se situe à l'extérieur de la frontière RGT.
Dérangement (*trouble*)	[X.790] Toute cause pouvant conduire ou contribuer à la perception par un gestionnaire d'une dégradation de la qualité de service d'un ou de plusieurs réseaux gérés ou d'une ou de plusieurs ressources gérées.

Terme	Définition
Administration des dérangements (*trouble administration*)	[X.790] Ensemble de fonctions permettant de signaler des dérangements et de suivre leur statut. L'administration des dérangements comprend la demande de format de dossier de dérangement, la saisie du dossier de dérangement, l'addition d'information concernant un dérangement, la résiliation d'un dossier de dérangement, l'examen de l'historique de dérangement, la notification de changement d'attribut (par exemple pour le statut du dossier de dérangement ou pour l'engagement de date), la création et la suppression de l'objet "dossier de dérangement", la vérification de l'achèvement de la réparation et la modification de l'information d'administration des dérangements.
Enregistrement d'historique de dérangement (*trouble history record*)	[X.790] Enregistrement d'informations sélectionnées à partir d'un dossier de dérangement, conservé à des fins d'historique après la fermeture du dossier de dérangement.
Gestion des dérangements (*trouble management*)	[X.790] Signalement et suivi d'erreur faits par des entités CME interagissant en coopération pour la résolution d'un dérangement (aucune distinction n'est faite entre des interfaces situées entre deux domaines de compétence ou à l'intérieur d'un même domaine de compétence).
Signalement de dérangement (*trouble reporting*)	[X.790] Acte de communication indiquant qu'un dérangement a été détecté de manière à permettre la mise en œuvre de la gestion des dérangements pour sa résolution.
Résolution du dérangement (*trouble resolution*)	[X.790] Processus de diagnostic et de réparation requis pour résoudre un problème. Ceci inclut le processus d'assignation de tâches de travail spécifiques ou la responsabilité générale de solder et de fermer le dossier de dérangement.
Suivi de dérangement (*trouble tracking*)	[X.790] La capacité de suivre l'avancement d'un dossier de dérangement depuis sa création jusqu'à sa fermeture.
Type de dérangement (*trouble type*)	[X.790] La description ou catégorie du dérangement détecté.
Confiance (*trust*)	[X.509] On peut dire d'une manière générale qu'une entité "fait confiance" à une autre entité si la première fait l'hypothèse que la deuxième se comportera exactement comme attendu (par la première). Il se peut que cette confiance s'applique uniquement pour une fonction donnée. Le rôle clé de la confiance dans ce cadre décrit la relation entre une entité effectuant l'authentification et une autorité; une entité sera certaine qu'elle peut faire confiance à l'autorité pour ne créer que des certificats valides et fiables. [X.810] On dit que l'entité X *fait confiance* à l'entité Y pour un ensemble d'activités si et seulement si l'entité X suppose que l'entité Y se comportera d'une certaine façon par rapport aux activités.
Entité de confiance (*trusted entity*)	[X.810] Entité qui peut violer une politique de sécurité, soit en réalisant des actions qu'elle n'est pas censée accomplir, soit en ne réussissant pas à réaliser des actions qu'elle est censée accomplir.
Fonctionnalité de confiance (*trusted functionality*)	[X.800] Fonctionnalité perçue comme correcte en ce qui concerne certains critères, tels que ceux qui sont définis par une politique de sécurité, par exemple.
Tierce partie de confiance (*trusted third party*)	[X.810] Autorité de sécurité ou son agent auquel il est fait confiance au regard de certaines activités liées à la sécurité (dans le contexte d'une politique de sécurité).

Terme	Définition
Entité de confiance inconditionnelle (*unconditionally trusted entity*)	[X.810] Entité de confiance qui peut violer une politique de sécurité sans être détectée.
Utilisateur (*user*)	[M.3010] Personne physique ou procédé utilisant des services de gestion dans le but de réaliser des opérations de gestion.
Elément frontière du domaine visité (*visited border element*)	[H.530] Elément frontière (BE) situé dans le domaine visité.
Poste de travail (*workstation*)	[M.3010] Bloc physique qui exécute les fonctions de poste de travail (WSF).
Fonction de poste de travail (*workstation function*)	[M.3010] Bloc de fonctions qui interprète les informations du RGT pour l'utilisateur (homme), et vice versa.
Interface X (*X interface*)	[M.3010] Interface appliquée à des points de référence x.
Point de référence x (*x reference point*)	[M.3010] Point de référence situé entre des blocs OSF dans des RGT différents. (Note – Les entités situées au-delà du point de référence x peuvent faire partie d'un RGT (OSF) réel ou faire partie d'un environnement non RGT (du type OSF). Cette classification n'est pas visible au point de référence x.)
Certificat X.509 (*X.509 certificate*)	[J.170] Spécification de certificat de clé publique élaborée dans le cadre de la norme d'annuaire X.500 de l'UIT-T.

A.3 Autres sources de termes et définitions de l'UIT-T

La base de données en ligne de l'UIT-T SANCHO (*Sector Abbreviations and defiNitions for a teleCommunications tHesaurus Oriented*) donne accès aux "termes et définitions" ou aux "abréviations et acronymes" en anglais, français et espagnol définis dans les publications de l'UIT-T. Elle est accessible en ligne gratuitement à l'adresse www.itu.int/sancho. Une version CD-ROM est également publiée régulièrement. SANCHO contient l'ensemble des termes et des définitions ci-dessus accompagnés de la liste des Recommandations où le terme ou la définition est utilisé.

La CE 17 de l'UIT-T a élaboré un recueil de définitions relatives à la sécurité utilisées dans les Recommandations de l'UIT-T, accessible à l'adresse www.itu.int/ITU-T/studygroups/com17/cssecurity.html.

Annexe B: Catalogue des Recommandations de l'UIT-T incluant des aspects de sécurité

B.1 Aspects de sécurité traités dans le présent Manuel

F.400 *Aperçu général du système et du service de messagerie*

Cette Recommandation donne un aperçu permettant de définir globalement le système et le service d'un MHS et sert d'aperçu général du MHS. Cet aperçu s'insère dans un ensemble de Recommandations qui décrivent le modèle et les éléments de service du système et des services de messagerie (MHS). Cette Recommandation offre un aperçu des capacités d'un MHS qui sont utilisées par le fournisseur du service pour la fourniture de services de messagerie (MH, *message handling*) publics permettant aux utilisateurs d'échanger des messages selon le principe de l'enregistrement et de la retransmission. Le système de messagerie est conçu conformément aux principes du modèle de référence de l'interconnexion des systèmes ouverts (modèle de référence OSI) pour les applications de l'UIT-T (Recommandation X.200) et il utilise les services de la couche Présentation et les services fournis par d'autres éléments plus généraux du service d'application. Un MHS peut être constitué au moyen de tout réseau entrant dans le cadre OSI. Le service de transfert de messages assuré par le MTS est indépendant de l'application. Le service IPM (F.420 + X.420), le service de messagerie EDI (F.435 + X.435) et le service de messagerie vocale (F.440 + X.440) constituent des exemples d'application normalisée. Les systèmes d'extrémité peuvent utiliser le service de transfert de messages (MT, *message transfer*) pour des applications particulières définies par accord bilatéral. Les services de messagerie assurés par le fournisseur du service font partie du groupe de services télématiques. Les services publics construits sur le MHS ainsi que l'accès au MHS ou depuis le MHS pour les services publics sont définis dans les Recommandations de la série F.400. Les aspects techniques du MHS sont définis dans les Recommandations de la série X.400. L'architecture globale du système de messagerie est définie dans la Recommandation UIT-T X.402. Les éléments de service sont les caractéristiques de service fournies par les processus d'application. Les éléments de service sont considérés comme étant des composantes des services offerts aux utilisateurs et sont soit des éléments d'un service de base, ou des fonctionnalités optionnelles d'utilisateur, ces dernières étant classées en fonctionnalités principales d'utilisateur et en fonctionnalités additionnelles d'utilisateur. Les capacités de **sécurité** du MHS sont décrites au §.15/F.400, y compris les **menaces de sécurité** du MHS, le modèle de sécurité, les éléments de service décrivant les fonctionnalités de sécurité (définis dans l'Annexe B), la **gestion de la sécurité**, les effets liés à la sécurité du MHS, la sécurité du service IPM. Question 11/17

F.440 *Services de messagerie: le service de messagerie vocale (**VM**)*

Cette Recommandation décrit les caractéristiques générales d'exploitation et de qualité de service du service public international de messagerie vocale (**VM**, *voice messaging*), un type particulier de service de messagerie (MH) (*message handling*), qui est un service de télécommunication international offert par les Administrations et qui permet aux abonnés d'envoyer un message à un ou plusieurs destinataires et de recevoir des messages au moyen de réseaux de télécommunication utilisant conjointement des techniques d'enregistrement et de retransmission et des techniques d'enregistrement et interrogation. Le service de messagerie vocale permet aux abonnés de demander l'exécution de diverses fonctions pendant le traitement et l'échange de messages vocaux codés. Certaines fonctions sont propres au service de messagerie vocale de base. D'autres fonctions, qui ne sont pas des fonctions de base, peuvent, si elles sont fournies par les Administrations, être sélectionnées par l'usager pour chaque message ou pour une période convenue aux termes d'un contrat.

L'intercommunication avec le service de messagerie de personne à personne (IPM) (*interpersonal messaging*) peut être assurée en option dans le service de messagerie vocale. Il appartient aux Administrations de fournir les fonctions de base au niveau international. Les fonctions, autres que les fonctions de base, visibles pour l'abonné, sont classées en fonctions essentielles et fonctions supplémentaires. Les Administrations sont tenues de fournir les fonctions facultatives essentielles au niveau international. Certaines Administrations peuvent fournir des fonctions facultatives supplémentaires pour un usage national et sur le plan international sur la base d'accords bilatéraux. Les fonctions autres que les fonctions de base sont appelées fonctions facultatives d'usager. Il est possible d'assurer le service de messagerie vocale en empruntant un réseau de communication quelconque. Ce service peut être offert séparément ou en association avec divers services télématiques ou de transmission de données. Les spécifications techniques et les protocoles à utiliser dans le service de messagerie vocale sont définis dans les Recommandations de la série X.400.

Annexe G: Eléments de service de **sécurité** en messagerie vocale

Annexe H: Aperçu de la **sécurité** en messagerie vocale Question 11/17

F.851 *Télécommunications personnelles universelles – Description du service (ensemble de services 1)*

Cette Recommandation a pour but de fournir la description du service des télécommunications personnelles universelles (UPT) et de proposer des dispositions concernant son exploitation. Elle contient une description générale du service du point de vue de l'utilisateur ou abonné individuel des UPT. Ainsi, l'utilisateur UPT participe à un ensemble personnalisé de services souscrits par abonnement, à partir desquels il définit ses besoins personnels pour former le profil du service UPT. L'utilisateur UPT peut utiliser le service UPT avec un risque minimum de violation du secret ou de taxation erronée due à une utilisation frauduleuse. En principe, tout service de télécommunication de base peut être utilisé avec le service UPT. Les services fournis à l'utilisateur UPT sont limités uniquement par les réseaux et les terminaux utilisés. "L'authentification de l'identité de l'utilisateur UPT" est la première des fonctions essentielles d'utilisateur et l'authentification du fournisseur de service UPT constitue une fonctionnalité facultative d'utilisateur. Le § 4.4 traite des prescriptions de sécurité. Question 3/2

H.233 *Système de confidentialité pour les services audiovisuels*

Un système de protection des données privées comprend deux parties, le mécanisme de confidentialité ou processus de chiffrement des données et un sous-système de gestion de clés. Cette Recommandation décrit la partie mécanisme de confidentialité d'un système de protection des données privées destiné à être utilisé dans les services audiovisuels à bande étroite. Bien qu'un tel système de protection des données privées nécessite un algorithme de chiffrement, la spécification de cet algorithme n'est pas incluse ici: le système admet plusieurs algorithmes spécifiques. Le système de confidentialité est applicable aux liaisons point à point entre terminaux ou entre un terminal et un pont de conférence (MCU, *multipoint control unit*); son application peut être élargie au fonctionnement multipoint sans chiffrement dans le pont de conférence Question G/16

H.234 *Gestion des clés de chiffrement et système d'authentification pour les services audiovisuels*

Un système de chiffrement comprend deux parties, le mécanisme de confidentialité ou processus de chiffrement des données, et un sous-système de gestion de clés. Cette Recommandation décrit les méthodes d'authentification et de gestion des clés pour un système de chiffrement destiné à être utilisé dans les services audiovisuels à bande étroite. La confidentialité est assurée à l'aide de *clés secrètes*. Ces clés sont chargées dans le mécanisme de chiffrement du système de confidentialité et régissent la manière dont les données transmises sont chiffrées et déchiffrées. Si un tiers accède aux clés utilisées, le système de chiffrement n'est plus sûr. La maintenance des clés par les utilisateurs est donc un élément important de tout système de confidentialité. Trois méthodes pratiques de gestion des clés sont spécifiées dans cette Recommandation. Question G/16

H.235 *Sécurité et cryptage des terminaux multimédias de la série H (terminaux H.323 et autres terminaux de type H.245)*

Des communications sûres et en temps réel sur des réseaux non sûrs font généralement intervenir *l'authentification* et le *secret des communications* (chiffrement des données). Cette Recommandation décrit des améliorations apportées dans le cadre des services de conférence interactifs afin d'y introduire des services de sécurité tels que l'authentification des points d'extrémité et le secret des communications multimédias. Elle décrit l'infrastructure de sécurité et les techniques spécifiques de secret des communications à utiliser. Le procédé qui est proposé est applicable aussi bien aux simples conférences point à point qu'aux conférences point à multipoint, à partir de tous les terminaux faisant appel au protocole de commande H.245. Cette version (11/00) porte sur la cryptographie à courbe elliptique, des profils de sécurité (de type à simple mot de passe ou à signature numérique perfectionnée), des contre-mesures de sécurité (protection contre l'inondation du média), l'algorithme de cryptage avancé (AES), le service d'arrière, les identificateurs d'objet (voir le guide à l'usage des responsables de l'implémentation de la Rec. l'UIT-T H.323). Question G/16

H.235 Annexe F *Profil de sécurité hybride*

Cette annexe décrit un profil de sécurité hybride à base d'infrastructure de clés publiques (PKI, *public key infrastructure*), efficace et modulable, utilisant les signatures numériques de l'Annexe E/H.235 et le profil de sécurité élémentaire de l'Annexe D/H.235. Cette annexe est proposée à titre d'option. Les entités de sécurité H.323 (terminaux, portiers, passerelles, ponts MCU, etc.) peuvent implémenter ce profil de sécurité hybride pour améliorer la sécurité ou pour l'assurer en cas de nécessité. Dans ce contexte, "hybride" signifie que les procédures de sécurité des profils de signature de l'Annexe E/H.235 sont en fait appliquées avec une certaine souplesse et que les signatures numériques restent conformes aux procédures RSA. Les signatures numériques ne sont cependant utilisées qu'en cas de nécessité absolue; en conditions normales, ce sont les techniques de sécurité symétriques hautement efficaces du profil de sécurité élémentaire de l'Annexe D/H.235 qui seront employées. Ce profil de sécurité hybride est applicable à la téléphonie IP "mondiale" modulable; il n'est pas exposé aux limitations du profil de sécurité élémentaire simple de l'Annexe D/H.235, lorsqu'il est appliqué de manière stricte. De plus, il n'est pas exposé à certains inconvénients du profil de l'Annexe E/H.235 tels qu'un plus grand besoin de largeur de bande et de performance lorsqu'il est appliqué de manière stricte. Par exemple, le profil de sécurité hybride ne dépend pas de l'administration (statique) de secrets mutuellement partagés dans les bonds de différents domaines. Les utilisateurs peuvent donc très facilement choisir leur fournisseur de téléphonie IP. Le profil de sécurité accepte une certaine mobilité de l'utilisateur. Par ailleurs, il n'applique la cryptographie asymétrique avec signatures et certificats qu'en cas de nécessité, se limitant sinon aux techniques symétriques, plus simples et plus efficaces. Il assure la mise en tunnel des messages H.245 pour l'intégrité de ceux-ci. Il offre également des dispositions pour la non-répudiation des messages. Ce profil de sécurité hybride utilise le modèle acheminé par portier; il est fondé sur les techniques de mise en tunnel H.245. La prise en charge de modèles non acheminés par portier nécessite un complément d'étude. Question G/16

H.323 *Systèmes de communication multimédia en mode paquet (Annexe J: Sécurisation des dispositifs d'extrémité simples)*

Cette Recommandation décrit les terminaux et autres entités qui assurent des services en temps réel de communications audio, vidéo, de données et/ou multimédias sur des réseaux en mode paquet n'offrant pas nécessairement une qualité de service garantie. Seul le mode audio est obligatoire, les modes données et vidéo étant facultatifs; en cas de prise en charge de ces deux modes facultatifs, on doit pouvoir utiliser un mode de fonctionnement commun spécifié permettant l'interfonctionnement de tous les terminaux acceptant ce type de médias. Le réseau à commutation par paquets peut inclure des réseaux locaux, des réseaux d'entreprise, des réseaux métropolitains, des intraréseaux et des

interréseaux (y compris l'Internet), des connexions point à point, un seul segment de réseau ou un interréseau de plusieurs segments aux topologies complexes. Les entités peuvent donc utiliser des configurations point à point, multipoint ou de diffusion. Elles peuvent fonctionner avec des terminaux sur le RNIS-LB, sur le RNIS-BE, sur des réseaux LAN offrant une qualité de service garantie, sur le RTGC et/ou sur des réseaux sans fil et peuvent être intégrées dans des ordinateurs personnels ou implémentées dans des dispositifs autonomes tels que des visiophones. Question G/16

H.530 *Procédures de sécurité symétrique pour la mobilité des systèmes H.323 selon la Recommandation H.510*

Cette Recommandation porte sur des procédures de sécurité dans les environnements H.323 avec mobilité, notamment pour la Rec. UIT-T H.510, qui décrit la mobilité pour les systèmes et services multimédias H.323. Elle décrit en détail les procédures de sécurité pour la Rec. UIT-T H.510. Jusque-là, les capacités de signalisation de la Rec. UIT-T H.235 dans ses versions 1 et 2 sont conçues pour prendre en charge la sécurité dans des environnements H.323 essentiellement sans mobilité. Dans ces environnements et dans les systèmes multimédias, une mobilité limitée est possible dans des zones de portier; la Rec. UIT-T H.323 en général et la Rec. UIT-T H.235 en particulier ne permettent qu'une prise en charge très réduite de la sécurité des utilisateurs et des terminaux mobiles lorsqu'ils passent d'un domaine à un autre et que de nombreuses entités interviennent dans un environnement réparti avec mobilité, par exemple. Les scénarios H.323 avec mobilité décrits dans la Rec. UIT-T H.510 relatifs à la mobilité des terminaux étant souples et dynamiques, ils constituent une situation nouvelle, notamment du point de vue de la sécurité. Lorsqu'ils passent d'un domaine à un autre, les terminaux mobiles et les utilisateurs H.323 doivent être authentifiés par le domaine étranger visité. De même, les utilisateurs mobiles souhaitent avoir la preuve de la véritable identité du domaine visité. En outre, il peut aussi être utile d'obtenir la preuve de l'identité des terminaux en plus de l'authentification des utilisateurs. Par conséquent, une authentification mutuelle de l'utilisateur et du domaine visité est absolument nécessaire, l'authentification de l'identité du terminal étant facultative. D'une manière générale, l'utilisateur mobile n'est connu que du domaine de rattachement dans lequel il est abonné et un mot de passe lui est attribué; ainsi, le domaine visité ne connaît pas cet utilisateur au départ. En tant que tel, le domaine visité ne partage aucune relation de sécurité établie avec l'utilisateur mobile et le terminal mobile. Concernant l'authentification et l'autorisation de l'utilisateur mobile et du terminal mobile, le domaine visité pourrait déléguer certaines tâches liées à la sécurité, telles que les contrôles d'autorisation ou la gestion des clés, au domaine de rattachement via des entités de réseau et de service intermédiaires. Pour cela, il faut sécuriser les communications et la gestion des clés entre le domaine visité et le domaine de rattachement. En principe, les environnements H.323 avec mobilité sont plus ouverts que les réseaux H.323 fermés, mais il faut bien évidemment sécuriser aussi de façon appropriée les tâches liées à la gestion des clés. Par ailleurs, il faut aussi protéger contre toute altération malveillante les communications intra et interdomaines de mobilité. Question G/16

J.93 *Prescriptions d'accès conditionnel dans le réseau de distribution secondaire de la télévision numérique par câble*

Cette Recommandation définit les prescriptions relatives à l'accès aux données et à la confidentialité des données afin de protéger les signaux de télévision numériques MPEG transmis sur les réseaux de télévision par câble entre la tête de réseau câblée et l'abonné ultime. Les algorithmes cryptographiques exacts utilisés dans ce processus ne figurent pas dans la Recommandation J.93 car ils sont déterminés à l'échelle régionale et/ou par les industries. CE 9

J.96 Amd 1 *Méthode technique permettant de garantir la confidentialité des transmissions internationales longue distance de télévision MPEG-2 conformes à la Recommandation UIT-T J.89*

Cette Recommandation contient une norme commune relative à un système à accès conditionnel pour la transmission internationale longue distance de télévision numérique conformément au profil professionnel MPEG-2 (4:2:2). Elle décrit le système d'embrouillage de base compatible (BISS, *basic interoperable scrambling system*), fondé sur la spécification DVB-CSA et utilisant des clés fixes en langage clair appelées mots de session. Un autre mode rétrocompatible fournit un mécanisme supplémentaire permettant d'insérer des mots de session cryptés, tout en conservant, parallèlement, l'interopérabilité. Question 6/9

J.170 *Spécification de la sécurité sur IPCablecom (J.sec)*

Cette Recommandation définit l'architecture de sécurité, les protocoles, les algorithmes, les prescriptions fonctionnelles associées et des prescriptions techniques afin d'assurer la sécurité sur le réseau IPCablecom. Les services de sécurité d'authentification, de contrôle d'accès, d'intégrité du contenu de signalisation et du contenu média, de confidentialité et de non-répudiation doivent être assurés conformément aux définitions données dans cette Recommandation pour chacune des interfaces d'élément de réseau. CE 9

M.3010 *Principes des réseaux de gestion des télécommunications*

Cette Recommandation définit les architectures – fonctionnelle, informationnelle et physique – d'un réseau de gestion des télécommunications (RGT) et leurs éléments fondamentaux. Elle décrit les relations existant entre les trois architectures et établit un cadre permettant d'établir les conditions à remplir pour la spécification des architectures physiques d'un RGT à partir des architectures fonctionnelles et informationnelles. Seules certaines parties de cette Recommandation traitent de la sécurité. Cette Recommandation propose un modèle de référence logique en vue de la stratification de la fonction de gestion, l'architecture logique répartie en couches (LLA, *logical layered architecture*). Elle établit les modalités à appliquer pour démontrer la conformité et l'observance de RGT aux fins d'interopérabilité. Les spécifications du RGT comprennent l'aptitude à garantir un accès sûr à l'information de gestion par les utilisateurs autorisés. Le RGT inclut des blocs fonctionnels pour lesquels la fonctionnalité de sécurité est assurée par des techniques de sécurité visant à protéger l'environnement du RGT afin de garantir la sécurité des informations échangées aux interfaces et résidant dans l'application de gestion. Principes et mécanismes de sécurité sont liés au contrôle des droits d'accès des utilisateurs du RGT aux informations associées aux applications du RGT.
Question 7/4

M.3016 *Aperçu général de la sécurité du RGT (M.3sec)*

Cette 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 Recommandation M.3010. Elle est de nature générique et n'identifie ou ne concerne pas des prescriptions pour une interface de RGT spécifique. Question 7/4

M.3210.1 *Services de gestion RGT pour la gestion de la sécurité des réseaux IMT-2000*

Cette Recommandation fait partie de la série de Recommandations *Services de gestion du réseau de gestion des télécommunications* qui contient une description des services de gestion, des objectifs et du contexte des aspects liés à la gestion des réseaux IMT-2000. Elle s'appuie sur l'ensemble des fonctions identifiées dans la Rec. UIT-T M.3400 et définit des ensembles de fonctions, des fonctions et des paramètres nouveaux en y ajoutant des éléments sémantiques et limitations additionnelles. Elle décrit un sous-ensemble des services de gestion de la sécurité afin d'offrir des prescriptions et une analyse de la gestion de la sécurité ainsi qu'un profil de gestion des fraudes dans un réseau mobile IMT-2000. L'accès est mis sur l'interface X entre deux fournisseurs de services et sur les services de gestion nécessaires entre ces deux fournisseurs afin que ceux-ci puissent détecter et prévenir toute forme de fraude grâce au système de collecte des informations de fraude (FIGS, *fraud information gathering system*), qui leur permet de surveiller un ensemble défini d'activités d'abonné afin de limiter leurs risques financiers face à des factures impayées conséquentes produites par des comptes d'abonné pendant que ces abonnés se trouvent en situation d'itinérance. Question 14/4

M.3320 *Cadre général des prescriptions de gestion pour l'interface X du réseau de gestion des télécommunications*

Cette Recommandation fait partie d'une série qui traite du transfert d'informations pour la gestion des réseaux et des services de télécommunication et seules certaines parties portent sur des aspects de sécurité. Cette Recommandation a pour objet de définir un cadre général couvrant toutes les prescriptions liées aux fonctions, aux services et aux réseaux pour l'échange d'informations entre Administrations via le réseau de gestion des télécommunications (RGT). Elle fournit également le cadre général concernant l'utilisation de l'interface X du RGT pour l'échange d'informations entre des Administrations, des exploitations reconnues, d'autres opérateurs de réseaux, des prestataires de services, des clients et d'autres entités. Question 9/4

M.3400 *Fonctions de gestion du réseau de gestion des télécommunications*

Cette Recommandation fait partie d'une série de Recommandations sur le réseau de gestion des télécommunications (RGT). Elle spécifie les fonctions de gestion et les ensembles de fonctions de gestion d'un RGT. Son contenu vient à l'appui de la base d'information de Tâche B (*rôles, ressources et fonctions RGT*), associée à la Tâche 2 (*description du contexte de gestion RGT*) indiquée dans la Rec. UIT-T M.3020: Méthodologie pour la spécification des interfaces du réseau de gestion des télécommunications. Lorsqu'on effectuera l'analyse d'un contexte de gestion RGT, il sera souhaitable d'envisager une utilisation maximale des ensembles de fonctions RGT proposés dans cette Recommandation. Question 7/4

Q.293 *Délais au bout desquels il convient de prendre des mesures de sécurité*

Il s'agit d'un extrait du Livre Bleu, qui contient uniquement les § 8.5 (Délais au bout desquels il convient de prendre des mesures de sécurité) à 8.9 (Méthode de partage de la charge) de la Rec. UIT-T Q.293. CE 4

Q.813 *Elément de service d'application des transformations de sécurité pour l'élément de service d'opérations distantes (STASE-ROSE)*

Cette Recommandation fournit des spécifications pour la prise en charge de transformations de sécurité, telles que le chiffrement, le hachage, le scellé et la signature, en se concentrant sur l'unité de données protocolaires (PDU, *protocol unit data*) de l'élément de service d'opérations distantes (ROSE, *remote operations service element*) considérée comme un tout. Les transformations de sécurité sont utilisées pour fournir divers services de sécurité tels que l'authentification, la confidentialité, l'intégrité et la non-répudiation. La présente Recommandation décrit une démarche pour la fourniture de transformations de sécurité qui est mise en œuvre au niveau de la couche application et ne fait appel à aucune fonctionnalité spécifique de la sécurité dans l'une quelconque des couches sous-jacentes de la pile OSI. Question 18/4

Q.815 *Spécification d'un module de sécurité pour la protection globale des messages*

Cette Recommandation spécifie un module de sécurité facultatif à utiliser avec la Rec. UIT-T Q.814, Spécification d'un agent interactif d'échange informatisé de données, qui fournit des services de sécurité pour l'ensemble des unités de données protocolaires (PDU). Le module de sécurité prend notamment en charge la non-répudiation de l'origine et de la réception, ainsi que l'intégrité globale des messages. Question 18/4

Q.817 *Infrastructure des clés publiques du RGT – Profils des certificats numériques et des listes de révocation des certificats*

Cette Recommandation expose la manière dont les certificats numériques et les listes de révocation de ces certificats peuvent être utilisés dans le RGT et définit les conditions d'utilisation de ces extensions des certificats et listes. Elle est destinée à faciliter l'interopérabilité entre éléments RGT utilisant l'infrastructure de clé publique (PKI, *public key infrastructure*) dans le cadre des fonctions de sécurité. L'objet de cette Recommandation est d'offrir un mécanisme interopérable et modulable pour la distribution et la gestion de clés à l'intérieur d'un RGT, de part et d'autre de toutes les interfaces, ainsi que pour la prise en charge d'un service de non-répudiation à travers l'interface X. Cette Recommandation concerne toutes les interfaces et applications du RGT. Elle est indépendante de la pile de protocoles de communication ou du protocole de gestion de réseau utilisé. Les ressources de l'infrastructure PKI peuvent être utilisées dans une grande étendue de fonctions de sécurité comme l'authentification, l'intégrité, la non-répudiation et l'échange de clés (UIT-T M.3016). Cette Recommandation ne spécifie cependant pas la façon dont il convient d'implémenter de telles fonctions, avec ou sans infrastructure PKI. Question 18/4

Q.1531 *Prescriptions de sécurité dans les TPU pour l'ensemble de services 1*

Cette Recommandation spécifie les prescriptions de sécurité pour les télécommunications TPU concernant les communications entre l'utilisateur et le réseau ainsi qu'entre réseaux, qui s'appliquent à l'ensemble de services 1 des télécommunications TPU, tel qu'il est défini dans la Recommandation F.851. Cette Recommandation traite de toutes les caractéristiques de sécurité pour les télécommunications TPU utilisant des accès avec une signalisation multifréquence DTMF et les accès utilisateur basés sur la signalisation DSS1 hors bande. CE 15

Q.1741.1 *Références IMT-2000 à la version 1999 du réseau central UMTS issu du GSM avec réseau d'accès radioélectrique universel de Terre (UTRAN)*

Cette Recommandation contient des références aux spécifications suivantes du 3GPP relatives à la sécurité:

TS 21.133: Atteintes à la sécurité et exigences

TS 22.100: Phase 1 du système UMTS

TS 22.101: Principes du service UMTS

TS 33.102: Architecture de la sécurité

TS 33.103: Directives d'intégration de la sécurité

TS 33.105: Exigences relatives à l'algorithme cryptographique

TS 33.106: Exigences d'interception licite

TS 33.107: Architecture et fonctions d'interception licite

TS 33.120: Objectifs et principes de sécurité SSG

Q.1741.2 *Références IMT-2000 à la version 4 du réseau central UMTS issu du GSM avec réseau d'accès radioélectrique universel de Terre (UTRAN)*

Cette Recommandation contient des références aux spécifications suivantes du 3GPP relatives à la sécurité:

TS 21.133: Sécurité 3G; atteintes à la sécurité et prescriptions

TS 22.048: Mécanismes de sécurité pour l'utilitaire d'application de module (U)SIM; étape 1

TS 22.101: Aspects du service; principes de service

TS 33.102: Sécurité 3G; architecture

TS 33.103: Sécurité 3G; directives d'intégration

TS 33.105: Prescriptions relatives à l'algorithme cryptographique

TS 33.106: Prescriptions d'interception licite

TS 33.107: Sécurité 3G; architecture et fonctions d'interception licite

TS 33.120: Objectifs et principes de sécurité

TS 33.200: Sécurité dans le domaine du réseau; protocole MAP

TS 35.205, .206, .207, et .208: Sécurité 3G; spécification de l'ensemble algorithmique MILENAGE: exemple d'ensemble algorithmique pour l'authentification 3GPP et les fonctions de production de clés *f*1, *f*1*, *f*2, *f*3, *f*4, *f*5 et *f*5*; (.205: généralités; .206: spécification des algorithmes; .207: données d'essai du réalisateur; .208: données d'essai de conformité à la conception) CES

Q.1741.3 *Références IMT-2000 à la version 5 du réseau central UMTS issu du GSM avec réseau d'accès radioélectrique universel de Terre (UTRAN)*

Cette Recommandation contient des références aux spécifications suivantes du 3GPP relatives à la sécurité:

TS 22.101: Aspects du service; principes de service

TS 33.102: Sécurité 3G; architecture

TS 33.106: Prescriptions d'interception licite

TS 33.107: Sécurité 3G; architecture et fonctions d'interception licite

TS 33.108: Sécurité 3G; interface de transfert pour l'interception licite

TS 33.200: Sécurité dans le domaine du réseau; protocole MAP

TS 33.203: Sécurité 3G; sécurité d'accès pour les services IP

TS 33.210: Sécurité; sécurité dans le domaine du réseau; sécurité de la couche de réseau IP

TS 35.205, .206, .207, .208 et .909: Sécurité 3G; spécification de l'ensemble algorithmique MILENAGE: exemple d'ensemble algorithmique pour l'authentification 3GPP et les fonctions de production de clés *f*1, *f*1*, *f*2, *f*3, *f*4, *f*5 et *f*5*; (.205: généralités; .206: spécification des algorithmes; .207: données d'essai du réalisateur; .208: données d'essai de conformité à la conception; .909: récapitulation et résultats de conception et d'évaluation) CES

Q.1742.1 *Références IMT-2000 au réseau central évolué ANSI-41 avec réseau d'accès cdma2000*

Cette Recommandation associe les normes de réseau central publiées par des organisations de normalisation et les spécifications du projet 3GPP2 approuvées au 17 juillet 2001 pour le membre "Réseau central évolué ANSI-41 avec réseau d'accès cdma2000" de la famille des IMT-2000. Les spécifications du projet 3GPP2 approuvées jusqu'en juillet 2002 seront associées dans la future Rec. UIT-T Q.1742.2 aux normes de réseau central déjà publiées. L'interface radioélectrique, le réseau d'accès radioélectrique et les normes des organisations de normalisation pour ce membre de la famille des IMT-2000 sont associés dans la Rec. UIT-R M.1457. Les associations concernant d'autres membres de cette famille sont présentées dans les Recommandations UIT-T de la série Q.174x. Cette Recommandation réunit et associe en une seule les normes de réseau central établies par plusieurs organisations de normalisation pour ce membre de la famille des IMT-2000. CES

Q.1742.2 *Références IMT-2000 (approuvées au 11 juillet 2002) au réseau central évolué ANSI-41 avec réseau d'accès cdma2000*

Cette Recommandation associe les normes relatives au réseau central publiées par des organisations de normalisation (SDO, *standards development organization*) aux spécifications 3GPP2, approuvées au 11 juillet 2002, du "Réseau central évolué ANSI-41 avec réseau d'accès cdma2000" qui fait partie de la famille des IMT-2000. Les spécifications 3GPP2 approuvées au 17 juillet 2001 ont été associées dans la Rec. UIT-T Q.1742.1 aux normes de réseau central déjà publiées. Les spécifications 3GPP2 approuvées jusqu'en juillet 2003 seront associées dans la future Rec. UIT-T Q.1742.3 aux normes de réseau central déjà publiées. L'interface radioélectrique, le réseau d'accès radioélectrique et les normes des organisations de normalisation pour ce membre de la famille des IMT-2000 sont associés dans la Rec. UIT-R M.1457-1. Les associations concernant d'autres membres de cette famille sont présentées dans les Recommandations UIT-T de la série Q.174x. Cette Recommandation réunit et associe en un seul texte, les normes régionales relatives au réseau central de ce membre de la famille des IMT-2000.

CES

Q.1742.3 *Références IMT-2000 (approuvées au 30 juin 2003) au réseau central évolué ANSI-41 avec réseau d'accès cdma2000*

Les spécifications techniques suivantes citées dans la Recommandation Q.1742.3 portent sur des aspects de sécurité:

Spécifications intersystèmes:

- N.S0003-0 User Identity Module (Version 1.0; avril 2001)
- N.S0005-0 Cellular Radiotelecommunications Intersystem Operations (Version 1.0; pas de date)
- N.S0009-0 IMSI (Version 1.0; pas de date)
- N.S0010-0 Advanced features in Wideband Spread Spectrum Systems (Version 1.0; pas de date)
- N.S0011-0 OTASP and OTAPA (Version 1.0; pas de date)
- N.S0014-0 Authentication Enhancements (Version 1.0; pas de date)
- N.S0018 TIA/EIA-41-D Prepaid Charging (Version 1.0.0; 14 juillet 2000)
- N.S0028 Network Interworking Between GSM MAP and ANSI-41 MAP Rev. B Revision: 0 (Version 1.0.0; avril 2002)

Spécifications applicables aux données en mode paquet:

- P.S0001-A Wireless IP Network Standard (Version 3.0.0; 16 juillet 2001)
- P.S0001-B Wireless IP Network Standard (Version 1.0.0; 25 octobre 2002)

Spécifications des aspects services et système:

- S.R0005-B Network Reference Model for cdma2000 Spread Spectrum Systems Revision: B (Version 1.0; 16 avril 2001)
- S.R0006 Wireless Features Description Revision: 0 (Version 1.0.0; 13 décembre 1999)
- S.R0009-0 User Identity Module (Version 1.0; Stage 1) Revision: 0 (13 décembre 1999)
- S.R0018 Pre-Paid Charging (Version 1.0.0; Stage 1) Revision: 0 (13 décembre 1999)
- S.R0019 Location-Based Services System (Version 1.0.0; LBSS) Stage 1 Description (22 septembre 2000)
- S.R0032 Enhanced Subscriber Authentication (Version 1.0; ESA) and Enhanced Subscriber Privacy (ESP) (6 décembre 2000)
- S.R0037-0 IP Network Architecture Model for cdma2000 Spread Spectrum Systems (Version 2.0; 14 mai 2002)

S.R0048 3G Mobile Equipment Identifier (Version 1.0; MEID) (10 mai 2001)

S.S0053 Common Cryptographic Algorithms (Version 1.0; 21 janvier 2002)

S.S0054 Interface Specification for Common Cryptographic Algorithms (Version 1.0; 21 janvier 2002)

S.S0055 Enhanced Cryptographic Algorithms (Version 1.0; 21 janvier 2002)

S.R0058 IP Multimedia Domain System Requirements (Version 1.0 ; 17 avril 2003)

S.R0059 Legacy MS Domain – Step 1 System Requirements (Version 1.0; 16 mai 2002)

S.R0066-0 IP Based Location Services Stage 1 Requirements (Version 1.0; 17 avril 2003)

S.R0071 Legacy System Packet Data Surveillance Requirements Stage 1 Requirements (Version 1.0; 18 avril 2002)

S.R0072 All IP Packet Data Surveillance Requirements Stage 1 Requirements (Version 1.0; 18 avril 2002)

S.R0073 Internet Over-the-Air Handset Configuration Management (Version 1.0; IOTA) Stage 1 (11 juillet 2002)

S.S0078-0 Common Security Algorithms (Version 1.0; 12 décembre 2002) CES

T.30 *Procédures pour la transmission de documents par télécopie sur le réseau téléphonique général commuté*

L'Annexe G contient des procédures pour la transmission sécurisée de documents de télécopie du Groupe 3 utilisant les systèmes HKM et HFX. L'Annexe H porte sur la sécurisation de la télécopie G3 sur la base de l'algorithme RSA. CE 16

T.36 *Capacités de sécurité à utiliser avec les télécopieurs du Groupe 3*

Cette Recommandation définit les deux solutions techniques indépendantes, fondées sur les algorithmes HKM/HFX40 et l'algorithme RSA, qui peuvent être appliquées afin d'assurer la sécurité des transmissions par télécopie. CE 16

T.123rev Annexe B *Connexions de transport étendues*

Cette annexe à la Recommandation T.123 révisée décrit un protocole de négociation de connexion (CNP, *connection negotiation protocol*) qui permet de négocier les capacités de sécurité. Le mécanisme de sécurité appliqué inclut divers moyens permettant d'assurer la sécurité de réseau et de transport nœud par nœud (par exemple TLS/SSL, IPSEC sans IKE ou gestion de clés manuelle, X.274/ ISO TLSP et GSS-API). Question 1/16

T.503 *Profil d'application de document pour le transfert de documents de télécopie du Groupe 4*

Cette Recommandation définit un profil d'application de document qui peut être utilisé par n'importe quel service télématique. Elle a pour objet de spécifier un format d'échange applicable à l'échange de documents de télécopie du Groupe 4 ne contenant que des graphiques en points. Les documents sont échangés sous une forme formatée, qui permet au destinataire d'afficher et d'imprimer le document comme l'a prévu l'expéditeur. CE 16

T.563 *Caractéristiques des télécopieurs du Groupe 4*

Cette Recommandation définit les aspects généraux des télécopieurs du Groupe 4 ainsi que l'interface avec le réseau physique. CE 16

T.611 *Interface de communication programmable **APPLI/COM** pour les services de télécopie du Groupe 3, de télécopie du Groupe 4, télétex, télex, de messagerie électronique et de transfert de fichiers*

Cette Recommandation définit l'interface de communication programmable (PCI) appelée «**APPLI/COM**», assurant un accès unifié à différents services de télécommunication tels que le service de télécopie du Groupe 3 ou d'autres services de télématique. Elle décrit la structure et le contenu des messages ainsi que le procédé d'échange entre deux entités (à savoir l'application locale et l'application de communication). *Toute communication est précédée par un processus d'ouverture de session et se termine par un processus de fermeture de session. Ces deux processus facilitent l'implémentation de schémas de sécurité qui sont particulièrement importants dans les systèmes multi-utilisateurs. Ils permettent aussi d'implémenter des mécanismes de sécurité entre l'application locale et l'application de communication.* Cette Recommandation constitue une **API** (interface de programmation d'application) de haut niveau qui occulte toutes les particularités de télécommunication, mais donne aux concepteurs d'applications un puissant moyen de commande et de surveillance des activités de télécommunication. CE 8

X.217 *Technologies de l'information – Interconnexion des systèmes ouverts – Définition de service applicable à l'élément de service de contrôle d'association*

Cette Recommandation définit les services applicables à l'élément de service de contrôle d'association (**ACSE**) nécessaires au contrôle d'association d'application dans un environnement OSI. L'ACSE prend en charge deux modes de communication: connexion et sans connexion. Trois unités fonctionnelles sont définies dans l'ACSE. L'unité fonctionnelle noyau obligatoire sert à établir des associations d'application et à y mettre fin. L'ACSE inclut deux unités fonctionnelles facultatives, l'une d'elles étant l'unité fonctionnelle authentification, qui fournit des moyens supplémentaires permettant l'échange d'informations destinées à l'authentification lors de l'établissement d'une association sans ajouter de services. On peut recourir aux facilités d'authentification ACSE pour disposer d'une catégorie limitée de méthodes d'authentification.

Amendement 1: Prise en charge des mécanismes d'authentification en mode sans connexion.
Question 11/17

X.227 *Technologies de l'information – Interconnexion des systèmes ouverts – Protocole en mode connexion applicable à l'élément de service de contrôle d'association: spécification du protocole.*

Cette Spécification de protocole définit les procédures applicables à des instances de communication entre des systèmes qui désirent s'interconnecter dans un environnement OSI en mode connexion, c'est-à-dire un protocole en mode connexion applicable à l'élément de service d'application pour le contrôle d'association d'application, l'élément de service de contrôle d'association (**ACSE**). Cette Spécification de protocole inclut l'unité fonctionnelle noyau qui est utilisée pour établir les associations d'application et y mettre fin. L'unité fonctionnelle d'authentification offre des fonctions supplémentaires qui permettent l'échange d'informations destinées à assurer l'authentification pendant l'établissement de l'association sans que soient ajoutés de nouveaux services. Les fonctions d'authentification de l'élément ACSE peuvent être utilisées pour la prise en charge d'une classe limitée de méthodes d'authentification. L'unité fonctionnelle de négociation du contexte d'application offre des fonctions supplémentaires qui permettent le choix du contexte d'application pendant l'établissement de l'association. Cette Spécification de protocole comprend une annexe qui décrit une machine

protocolaire, appelée machine protocolaire de contrôle d'association (ACPM, *association control protocol machine*), en termes d'une table d'états. Elle comprend aussi une annexe qui décrit un mécanisme d'authentification simple utilisant un mot de passe avec une appellation AE et destiné à l'usage du public et qui contient aussi un exemple de spécification de mécanisme d'authentification. Le nom suivant (de type de données ASN.1 OBJECT IDENTIFIER) est affecté à ce mécanisme d'authentification:

{joint-iso-itu-t(2) association-control(2) authentication-mechanism(3) password-1(1)}.

Pour ce mécanisme d'authentification, le mot de passe est la valeur d'authentification. Le type de données de valeur d'authentification doit être "chaîne graphique". Question 11/17

X.237 *Technologies de l'information – Interconnexion des systèmes ouverts – Protocole en mode sans connexion pour l'élément de service de contrôle d'association: Spécification du protocole*

L'Amendement 1 à cette Recommandation introduit le marqueur d'extension ASN.1 dans le module décrivant le protocole. Il améliore également la spécification du protocole sans connexion pour l'ACSE afin de permettre l'acheminement de paramètres d'authentification dans l'unité APDU A-UNIT-DATA. Question 11/17

X.257 *Technologies de l'information – Interconnexion des systèmes ouverts – Protocole en mode sans connexion de l'élément de service de contrôle d'association: formulaire de déclaration de conformité d'une instance de protocole*

Cette Recommandation décrit le formulaire de déclaration de conformité d'une instance de protocole (PICS) (*protocol implementation conformance statement*) applicable au protocole en mode sans connexion de l'élément de service de contrôle d'association (ACSE) (*association control service element*) qui est spécifié dans la Rec. UIT-T X.237. Le formulaire PICS représente, sous la forme de tableaux, les éléments obligatoires et optionnels du protocole en mode sans connexion de l'élément de service ACSE. Le formulaire PICS est utilisé pour indiquer les caractéristiques et options d'une instance particulière du protocole en mode sans connexion de l'élément de service ACSE.
Question 11/17

X.272 *Compression et secret des données dans les réseaux à relais de trames*

Cette Recommandation définit le service de compression et de secret des données dans les réseaux à relais de trames, y compris la négociation et l'encapsulation de la compression de données, de la compression sécurisée de données, de l'authentification et du cryptage en relais de trames. La présence d'un service de compression de données dans un réseau augmentera le débit effectif de celui-ci. La demande en transmission de données sensibles sur des réseaux publics nécessite des ressources permettant d'assurer le secret de ces données. Afin d'obtenir des taux de compression optimaux, il est essentiel de comprimer les données avant de les crypter. Il est donc souhaitable d'offrir, dans la spécification du service de compression des données, des ressources permettant de négocier également des protocoles de cryptage des données. Etant donné que la tâche de compression puis de cryptage des données exige beaucoup de ressources de calcul, certains protocoles ont été proposés afin d'assurer simultanément la compression des données et leur cryptage (compression de données sécurisée). Les protocoles de compression de données sont fondés sur le protocole de commande de liaison PPP (IETF RFC 1661) et sur le protocole de commande de cryptage PPP (IETF RFC 1968 et 1969). Cette Recommandation s'applique aux trames d'information non numérotée (UI, *unnumbered information*) encapsulées conformément à l'Annexe E/Q.933. Elle traite de la compression et du secret des données sur connexions virtuelles permanentes (PVC, *permanent virtual connection*) comme sur connexions virtuelles commutées (SVC, *switched virtual connection*). Question 10/17

X.273 *Technologies de l'information – Interconnexion des systèmes ouverts – Protocole de sécurité de la couche réseau*

Cette Recommandation spécifie le protocole pouvant prendre en charge les services d'intégrité, de confidentialité, d'authentification et de contrôle d'accès identifiés dans le modèle de sécurité OSI comme applicables aux protocoles de couche réseau en mode connexion et en mode sans connexion. Le protocole prend en charge ces services au moyen de mécanismes cryptographiques, d'étiquetages de sécurité et d'attributs (clés de chiffrement par exemple) préétablis par la gestion de sécurité.
Question 11/17

X.274 *Technologies de l'information – Télécommunication et échange d'informations entre systèmes – Protocole de sécurité de la couche transport*

Cette Recommandation spécifie le protocole pouvant prendre en charge les services d'intégrité, de confidentialité, d'authentification et de contrôle d'accès identifiés dans le modèle de sécurité OSI comme relevant de la couche transport. Le protocole prend en charge ces services au moyen de mécanismes cryptographiques, d'étiquetages de sécurité et d'attributs (clés de chiffrement par exemple) préétablis par la gestion de sécurité. Question 11/17

X.400/F.400 *Services de messagerie: Aperçu général du système et du service de messagerie*

Cette Recommandation définit les éléments de service du système de messagerie (MHS) pour les services de **sécurité** suivants entre deux agents d'utilisateur, entre deux agents de transfert de messages, entre un agent d'utilisateur et un agent de transfert de message ainsi qu'entre un agent d'utilisateur et une mémoire de messages: confidentialité, intégrité, authentification, non-répudiation et contrôle d'accès, services identifiés comme se rapportant à la couche application. (Voir F.400)
Question 11/17

X.402 *Technologies de l'information – Systèmes de messagerie: Architecture globale*

Cette Recommandation spécifie les procédures de sécurité et les identificateurs d'objet à utiliser dans les protocoles MHS pour réaliser les services de confidentialité, d'intégrité, d'authentification, de non-répudiation et de contrôle d'accès identifiés comme se rapportant à la couche application.
Question 11/17

X.411 *Technologie de l'information – Systèmes de messagerie – Système de transfert de messages: définition et procédures du service abstrait*

Cette Recommandation spécifie les mécanismes et les procédures prenant en charge les services de confidentialité, d'intégrité, d'authentification et de non-répudiation identifiés comme se rapportant à la couche application. Le protocole prend en charge ces services en utilisant des mécanismes cryptographiques, un étiquetage de sécurité et des signatures numériques, présentés dans la Recommandation X.509. Cette Recommandation spécifie un protocole qui utilise des techniques de chiffrement asymétrique, mais les techniques de chiffrement symétrique sont également prises en charge. Question 11/17

X.413 *Technologies de l'information – Systèmes de messagerie: mémoire de messages: définition du service abstrait*

Cette Recommandation spécifie les mécanismes, le protocole et les procédures prenant en charge les services d'intégrité, de contrôle d'accès, d'authentification et de non-répudiation identifiés comme se rapportant à la couche application. Le protocole prend en charge ces services pour le compte de l'utilisateur direct de la mémoire de messages. Question 11/17

X.419 *Technologies de l'information – Systèmes de messagerie: Spécification des protocoles*

Cette Recommandation spécifie les procédures et les contextes d'application permettant d'assurer un accès sécurisé aux entités et utilisateurs distants du système de messagerie grâce à la prise en charge des services d'authentification et de contrôle d'accès identifiés comme se rapportant à la couche application. Question 11/17

X.420 *Technologies de l'information – Systèmes de messagerie: système de messagerie de personne à personn*

Cette Recommandation spécifie les mécanismes, le protocole et les procédures applicables à l'échange d'objets entre utilisateurs de la messagerie de personne à personne ou agents d'utilisateur pour le compte de l'utilisateur direct. Les services de sécurité pris en charge sont l'intégrité, la confidentialité, l'authentification et le contrôle d'accès identifiés comme se rapportant à la couche application.
Question 11/17

X.435 *Technologies de l'information – Systèmes de messagerie: système de messagerie par échange informatisé de données*

Cette Recommandation spécifie les mécanismes, le protocole et les procédures applicables à l'échange d'objets entre agents d'utilisateur de l'échange informatisé de données (EDI) pour le compte de l'utilisateur direct. Les services de sécurité pris en charge sont l'intégrité, la confidentialité, l'authentification et le contrôle d'accès identifiés comme se rapportant à la couche application.
Question 11/17

X.440 *Technologies de l'information – Systèmes de messagerie: système de messagerie vocale*

Cette Recommandation spécifie les mécanismes, le protocole et les procédures applicables à l'échange d'objets entre agents d'utilisateur de la messagerie vocale pour le compte de l'utilisateur direct. Les services de sécurité pris en charge sont l'intégrité, la confidentialité, l'authentification et le contrôle d'accès identifiés comme se rapportant à la couche application. Question 11/17

X.500 *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: aperçu général des concepts, modèles et services*

Cette Recommandation spécifie l'annuaire et ses caractéristiques de sécurité. Question 9/17

X.501 *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: les modèles*

Cette Recommandation spécifie l'utilisation du cadre général des certificats de clé publique et d'attribut X.509 de l'annuaire. Question 9/17

X.509 *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire:*

---- Cadre d'authentification (édition de 1993 – deuxième édition/version)

---- Cadre d'authentification (édition de 1997 – troisième édition/version)

---- Cadre général des certificats de clé publique et d'attribut (édition de 2000 – quatrième édition/version)

Cette Recommandation définit un cadre général des certificats de clé publique et d'attribut ainsi qu'un cadre pour la fourniture de services d'authentification de l'annuaire au bénéfice de ses utilisateurs. Elle décrit deux niveaux d'authentification, l'authentification simple utilisant un mot de passe pour vérifier l'identité déclarée et l'authentification forte nécessitant des justificatifs créés au moyen de méthodes de chiffrement. L'authentification simple fournit une certaine protection contre les accès non autorisés, mais seule l'authentification forte devrait être utilisée pour fournir la base de services fiables. Les

cadres définis peuvent être utilisés pour définir un profil d'application d'infrastructures de clé publique (**PKI**) et d'infrastructures de gestion de privilège (**PMI**). Le cadre des certificats de clé publique comprend la spécification des objets de données utilisés pour représenter les certificats proprement dits ainsi que les notifications de révocation de certificats émis et auxquels il ne doit plus être fait confiance. Il définit certains composants critiques d'une infrastructure de clé publique (**PKI**), mais pas la totalité d'une telle infrastructure. Toutefois, il constitue une base permettant d'édifier des infrastructures **PKI** complètes et leurs spécifications. Le cadre des certificats d'attribut contient la spécification des objets de données utilisés pour représenter les certificats proprement dits, ainsi que les notifications de révocation de certificat émis auxquels il ne doit plus être fait confiance. Il définit certains composants critiques d'une infrastructure de gestion de privilège (**PMI**), mais pas la totalité d'une telle infrastructure. Toutefois, il constitue une base permettant d'édifier des infrastructures **PMI** complètes et leurs spécifications. Sont définis également les *objets d'informations* permettant de stocker les objets d'infrastructure PKI et PMI dans l'annuaire et de comparer des valeurs présentées avec les valeurs stockées. Question 9/17

X.519 *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: spécification des protocoles*

Cette Recommandation spécifie les procédures et les contextes d'application permettant d'assurer un accès sécurité au cours du rattachement d'entités d'annuaire. Question 9/17

X.733 *Technologies de l'information – Interconnexion de systèmes ouverts – Gestion des systèmes: fonction de signalisation des alarmes*

Cette Recommandation définit une fonction de gestion des systèmes interactive qui peut être utilisée par un processus d'application dans le contexte d'une gestion centralisée ou décentralisée. Elle définit une fonction qui se compose de définitions génériques, de services et d'unités fonctionnelles et qui s'inscrit dans la couche application du modèle de référence OSI. Les notifications d'alarme définies par cette fonction fournissent l'information dont peut avoir besoin le gestionnaire des systèmes pour réagir selon les conditions d'exploitation et la qualité de service propre à un système. Question 17/4

X.735 Technologie de l'information – Interconnexion de systèmes ouverts – Gestion des systèmes: fonction de commande des registres de consignation

Cette Recommandation définit une fonction de gestion des systèmes qui peut être utilisée par un processus d'application dans un environnement de gestion centralisée ou décentralisée aux fins de la gestion des systèmes. Elle définit la fonction de commande des registres de consignation (fonction de commande de consignation) au moyen de services et de deux unités fonctionnelles. Cette fonction se situe dans la couche application. Question 17/4

X.736 *Technologies de l'information – Interconnexion de systèmes ouverts – Gestion des systèmes: fonction de signalisation des alarmes de sécurité*

Cette Recommandation | Norme internationale définit la fonction de signalisation des alarmes de sécurité. Cette fonction est une fonction de gestion des systèmes qui peut être utilisée par un processus d'application dans un environnement de gestion centralisée ou décentralisée pour échanger des informations destinées à la gestion des systèmes, telle qu'elle est définie dans la Recommandation X.700 du CCITT | ISO/CEI 7498-4. Cette Recommandation | Norme internationale intervient dans la couche application spécifiée dans la Recommandation X.200 | ISO 7498; elle est définie selon le modèle fourni dans la Norme ISO/CEI 9545. Le rôle des fonctions de gestion des systèmes fait l'objet de la Recommandation X.701 du CCITT | ISO/CEI 10040. Les notifications d'alarme de sécurité définies par cette fonction de gestion des systèmes fournissent des informations concernant l'état opérationnel et la qualité de service concernant la sécurité. Question 14/4

X.740 *Technologie de l'information – Interconnexion de systèmes ouverts – Gestion des systèmes: fonction de piste de vérification de sécurité*

Cette Recommandation | Norme internationale définit la fonction de piste de vérification de sécurité. Il s'agit d'une fonction de gestion des systèmes qui peut être utilisée par un processus d'application dans un environnement de gestion centralisée ou décentralisée afin d'échanger les informations et commandes de gestion des systèmes, telle qu'elle est définie dans la Rec. X.700 du CCITT | ISO/CEI 7498-4. Cette Recommandation | Norme internationale se situe dans la couche application de la Rec. X.200 du CCITT | ISO 7498; elle est définie conformément au modèle fourni par ISO/CEI 9545. Le rôle des fonctions de gestion des systèmes est décrit dans la Rec. X.701 du CCITT | ISO/CEI 10040. Question 14/4

X.741 *Technologies de l'information – Interconnexion des systèmes ouverts – Gestion-systèmes: objets et attributs de contrôle d'accès*

Cette Recommandation | Norme internationale spécifie un modèle de sécurité pour le contrôle d'accès ainsi que les informations de gestion qui sont nécessaires afin de créer et d'administrer le contrôle d'accès associé à la gestion des systèmes OSI. La politique de sécurité adoptée dans chaque instance d'utilisation n'est pas spécifiée et est laissée aux soins des réalisateurs. Cette Spécification est générique et applicable à la gestion de la sécurité de nombreux types d'application. Question 14/4

X.800 *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT*

Cette Recommandation définit les éléments généraux d'architecture ayant trait à la sécurité, que l'on peut appliquer de façon appropriée dans les cas où une protection de la communication entre systèmes ouverts est requise. Dans le cadre du modèle de référence, elle établit des principes directeurs et des contraintes permettant d'améliorer les Recommandations existantes ou d'élaborer de nouvelles Recommandations dans le contexte de l'OSI pour permettre des communications sûres et donner ainsi une approche cohérente de la sécurité dans l'OSI. Cette Recommandation est une extension du modèle de référence destinée à couvrir les aspects de sécurité qui sont des éléments généraux d'architecture des protocoles de communication, mais qui ne sont pas traités dans le modèle de référence. Cette Recommandation donne une description générale des services de sécurité et des mécanismes associés qui peuvent être fournis par le modèle de référence et signale, dans le modèle de référence, les emplacements où les services et mécanismes peuvent être fournis. Question 10/17

X.802 *Technologies de l'information – Modèle de sécurité des couches inférieures*

Cette Recommandation décrit les aspects intercouches de la fourniture des services de sécurité dans les couches inférieures du Modèle de référence OSI (couches transport, réseau, liaison de données et physique). Elle décrit les concepts architecturaux communs à ces couches, la base des interactions entre couches relatives à la sécurité, et le positionnement des protocoles de sécurité dans les couches inférieures. Question 10/17

X.803 *Technologies de l'information – Interconnexion des systèmes ouverts – Modèle de sécurité pour les couches supérieures*

Cette Recommandation décrit la sélection, l'insertion et l'utilisation des services et mécanismes de sécurité dans les couches supérieures (application, présentation et session) du Modèle de référence OSI. Question 10/17

X.805 *Architecture de sécurité pour les systèmes assurant des communications de bout en bout*

Cette Recommandation définit les éléments généraux d'architecture ayant trait à la sécurité, qui, lorsqu'ils sont mis en œuvre comme il convient, en particulier dans un environnement multifabricants, garantissent qu'un réseau est correctement protégé contre les attaques malveillantes et contre celles qui se produisent par inadvertance, qu'il présente une grande disponibilité et des délais de réponse appropriés, qu'il est intègre et évolutif et qu'il comporte une fonction de facturation précise.

Question 10/17

X.810 *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: aperçu général*

Cette Recommandation définit le cadre dans lequel les services de sécurité pour les systèmes ouverts sont spécifiés. Cette partie des cadres de sécurité définit l'organisation du cadre de sécurité, définit les concepts de sécurité requis dans plusieurs parties des cadres de sécurité, et décrit les interrelations des services et mécanismes identifiés dans les autres parties du cadre. Ce cadre décrit tous les aspects d'authentification tels qu'ils s'appliquent aux systèmes ouverts, la relation entre l'authentification et d'autres fonctions de sécurité comme le contrôle d'accès et les besoins de gestion pour l'authentification. Question 10/17

X.811 *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour systèmes ouverts: cadre d'authentification*

Cette Recommandation définit un cadre général pour la fourniture de l'authentification. L'authentification vise essentiellement à contrer les menaces d'usurpation d'identité et de réexécution. Question 10/17

X.812 *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: cadre de contrôle d'accès*

Cette Recommandation définit un cadre général pour la fourniture du contrôle d'accès. Le but essentiel du contrôle d'accès est de parer au risque d'opérations non autorisées au moyen d'un ordinateur ou d'un système de communication; ces menaces sont fréquemment subdivisées en classes qui sont notamment les suivantes: utilisation non autorisée, divulgation, modification, destruction et déni de service. Question 10/17

X.813 *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité dans les systèmes ouverts: non-répudiation*

Cette Recommandation définit un cadre général pour la fourniture d'un service de non-répudiation. Le service de non-répudiation a pour objet de collecter, de conserver, de diffuser et de valider des preuves irréfutables concernant l'identification des expéditeurs et des destinataires participant à des transferts de données. Question 10/17

X.814 *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: cadre de confidentialité*

Cette Recommandation définit un cadre général pour la fourniture de services de confidentialité. La confidentialité est une propriété selon laquelle aucune information n'est communiquée ou divulguée à des individus, entités ou processus non autorisés. Question 10/17

X.815 *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: cadre d'intégrité*

Cette Recommandation définit un cadre général pour la fourniture de services d'intégrité. La propriété caractérisant des données qui n'ont pas été altérées ou détruites d'une manière non autorisée est appelée «intégrité». Question 10/17

X.816 *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: cadre d'audit et d'alarmes de sécurité*

Cette Recommandation décrit un modèle de base permettant de manipuler les alarmes de sécurité et de conduire un audit de sécurité pour les systèmes ouverts. Un audit de sécurité est une analyse et un examen – effectués de façon indépendante – des enregistrements et activités du système. Le service d'audit de sécurité fournit à une autorité d'audit la capacité de spécifier, sélectionner et gérer les événements qui doivent être enregistrés dans un journal d'audit de sécurité. Question 10/17

X.830 *Technologies de l'information – Interconnexion des systèmes ouverts – Sécurité générique des couches supérieures: aperçu général, modèles et notation*

Cette Recommandation fait partie d'une série de Recommandations comprenant un ensemble de moyens destinés à la réalisation des protocoles des couches supérieures de l'OSI qui prennent en charge les services de sécurité. Elle définit: a) des modèles généraux de fonctions de protocole d'échanges de sécurité et des transformations de sécurité; b) une série d'outils de notation pour spécifier les besoins de protection sélective des champs dans une spécification de syntaxe abstraite, les échanges de sécurité et les transformations de sécurité; c) une série de lignes directrices informatives sur l'application des moyens de sécurité génériques des couches supérieures traités dans cette série de Recommandations. Question 10/17

X.831 *Technologies de l'information – Interconnexion des systèmes ouverts – Sécurité générique des couches supérieures: définition du service assuré par l'élément de service d'échange de sécurité*

Cette Recommandation fait partie d'une série de Recommandations comprenant un ensemble de moyens destinés à la réalisation des protocoles des couches supérieures de l'OSI qui prennent en charge les services de sécurité. Elle spécifie le service fourni par l'élément de service d'échange de sécurité (SESE) qui est un élément de service d'application (ASE) facilitant la communication des informations nécessaires pour assurer les services de sécurité dans la couche application de l'OSI.
Question 10/17

X.832 *Technologies de l'information – Interconnexion des systèmes ouverts – Sécurité générique des couches supérieures: spécification du protocole d'élément de service d'échange de sécurité*

Cette Recommandation fait partie d'une série de Recommandations comprenant un ensemble de moyens destinés à la réalisation des protocoles des couches supérieures de l'OSI qui prennent en charge les services de sécurité. Elle spécifie le protocole fourni par l'élément de service d'échange de sécurité (SESE) qui est un élément de service d'application (ASE) facilitant la communication des informations nécessaires pour assurer les services de sécurité dans la couche application de l'OSI.
Question 10/17

X.833 *Technologies de l'information – Interconnexion des systèmes ouverts – Sécurité générique des couches supérieures: spécification de la syntaxe de protection du transfert*

Cette Recommandation fait partie d'une série de Recommandations comprenant un ensemble de moyens destinés à la réalisation des protocoles des couches supérieures de l'OSI qui prennent en charge les services de sécurité. Elle spécifie la syntaxe de protection du transfert qui est utilisée en association avec la couche présentation pour assurer des services de sécurité dans la couche application. Question 10/17

X.834 *Technologies de l'information – Interconnexion des systèmes ouverts – Sécurité générique des couches supérieures: formulaire de déclaration de conformité d'instance de protocole de l'élément de service d'échange de sécurité*

Cette Recommandation fait partie d'une série de Recommandations sur la sécurité générique des couches supérieures (GULS, *generic upper layers security*). Elle contient le formulaire de déclaration de conformité d'instance de protocole (PICS, *protocol implementation conformance statement*) pour le protocole d'élément de service d'échange de sécurité spécifié dans la Rec. UIT-T X.832 et pour les échanges de sécurité décrits dans l'Annexe C de la Rec. UIT-T X.830. Cette Recommandation décrit les capacités et options normalisées sous une forme qui permet l'évaluation, aux fins de conformité, d'une réalisation donnée. Question 10/17

X.835 *Technologies de l'information – Interconnexion des systèmes ouverts – Sécurité générique des couches supérieures: formulaire de déclaration de conformité d'instance de protocole de la syntaxe de protection du transfert*

Cette Recommandation fait partie d'une série de Recommandations sur la sécurité générique des couches supérieures (GULS, *generic upper layers security*). Elle contient le formulaire de déclaration de conformité d'instance de protocole (PICS, *protocol implementation conformance statement*) pour la spécification de la syntaxe de protection du transfert figurant dans la Rec. UIT-T X.833. Cette Recommandation décrit les capacités et options normalisées sous une forme qui permet l'évaluation, aux fins de conformité, d'une réalisation donnée. Question 10/17

X.841 *Technologies de l'information – Techniques de sécurité – Objets d'information de sécurité pour le contrôle d'accès*

Cette Recommandation sur les objets d'information de sécurité (SIO) pour le contrôle d'accès rassemble les définitions d'objets courantes utiles pour les normes de sécurité afin d'éviter la présence de définitions multiples et différentes de la même fonctionnalité. L'utilisation de la notation de syntaxe abstraite numéro un (ASN.1) a permis d'obtenir des définitions précises. Cette Recommandation ne couvre que les aspects statiques des objets d'information de sécurité (SIO). Question 10/17

X.842 *Technologies de l'information – Techniques de sécurité – Lignes directrices pour l'utilisation et la gestion des services de tiers de confiance*

Cette Recommandation traite des services qui ont recours à des tiers de confiance (TTP). Elle propose des lignes directrices sur leur utilisation et sur la gestion des services, une définition claire des responsabilités et des services de base, la description et l'objet de ceux-ci, ainsi que les rôles et les responsabilités des TTP et des entités qui font appel à leurs services. Elle distingue les différentes catégories de services TTP, notamment l'horodatage, la non-répudiation, la gestion de clés, la gestion de certificats et le notaire électronique. Question 10/17

X.843 *Technologies de l'information – Techniques de sécurité – Spécification de services de tiers de confiance (TTP) pour la prise en charge des applications de signature numérique*

Cette Recommandation définit les services nécessaires à la prise en charge des applications de signature numérique pour la non-répudiation de création d'un document. Comme cette prise en charge suppose que le document est intègre et que le créateur est authentique, les services décrits peuvent également être couplés aux services responsables de l'intégrité et de l'authenticité. Question 10/17

X.901 *Technologies de l'information – Traitement réparti ouvert – Modèle de référence: aperçu général*

La croissance rapide des applications réparties a fait naître le besoin d'un cadre pour coordonner la normalisation du traitement réparti ouvert (**ODP**, *open distributed processing*). Le modèle de référence ODP fournit ce cadre. Il établit une architecture qui permet la prise en compte de la répartition, de l'interfonctionnement et de la portabilité. Cette Recommandation contient un aperçu général du modèle de référence ODP, en précise les motivations, le domaine d'application et la justification, avec une explication des concepts clés ainsi qu'une présentation de l'architecture ODP. Elle explique la façon d'interpréter ce modèle de référence et la manière dont il peut être utilisé, en particulier par les rédacteurs de normes et par les architectes de systèmes ODP. Elle contient également une classification des domaines de normalisation en matière de systèmes répartis; cette classification s'appuie sur les points de référence de conformité identifiés dans la Rec. UIT-T X.903. Les systèmes ODP doivent être fiables, c'est-à-dire que leur construction et leur maintenance doit être telle que les services offerts par le système et les données qui lui sont confiées soient protégés contre

les accès non autorisés, les utilisations illicites et toute autre menace ou attaque. Il est plus difficile d'assurer le niveau de sécurité requis dès lors que les interactions ont lieu à distance et que des parties du système et ses utilisateurs sont mobiles. Les règles de sécurité pour les systèmes ODP peuvent définir: les règles applicables à la détection des menaces pesant sur la sécurité; les règles applicables à la protection contre les menaces pesant sur la sécurité; les règles applicables à la limitation des dommages causés par toute atteinte à la sécurité. Question 26/17

X.902 *Technologies de l'information – Traitement réparti ouvert – Modèle de référence: fondements*

Cette Recommandation définit les concepts et le cadre analytique servant à la description normalisée de systèmes (arbitraires) de traitement réparti. Elle introduit les principes de la conformité aux normes de traitement réparti ouvert (ODP) et la manière de les appliquer. Elle s'en tient à un niveau de détail suffisant pour les besoins de la Rec. X.903 et pour établir les prescriptions de nouvelles techniques de spécification. Question 26/17

X.903 *Technologies de l'information – Traitement réparti ouvert – Modèle de référence: architecture*

Cette Recommandation contient la spécification des caractéristiques requises pour qu'un système de traitement réparti puisse être qualifié d'ouvert: il s'agit des contraintes que doivent respecter les normes de traitement réparti ouvert (ODP, *open distributed processing*). Cette Recommandation utilise les techniques descriptives décrites dans la Recommandation X.902. Question 26/17

X.904 *Technologies de l'information – Traitement réparti ouvert – Modèle de référence: sémantique architecturale*

Cette Recommandation contient une normalisation des concepts de modélisation ODP définis aux § 8 et 9 de la Rec. UIT-T X.902. La normalisation est obtenue par l'interprétation de chaque concept en fonction des constructions des différentes techniques de description formelle normalisées.
Question 26/17

B.2 Aspects de sécurité non traités dans le présent Manuel (fiabilité et protection physique des installations extérieures)

La protection des installations extérieures contre la corrosion, les effets de l'environnement, les accidents causés par des incendies, les activités humaines et d'autres formes de dommages de tous les types de câble pour les télécommunications publiques et des structures associées, contribue à accroître la sécurité du transport d'informations du point de vue de la fiabilité et de la disponibilité des réseaux. La construction, l'installation et la surveillance des équipements et des câbles sont essentielles pour garantir le bon fonctionnement d'une liaison. Plus le volume d'informations transportées est grand, plus la protection physique d'une installation est importante. Les Recommandations de la série L décrivent des techniques permettant d'accroître la sécurité d'une installation et donc la sécurité des informations acheminées d'un site à un autre.

L.3 *Armure des câbles*

Pour les câbles en pleine terre, l'armure contribue à la sécurité de l'installation et du fonctionnement. Elle assure en effet la protection des câbles contre les accidents mécaniques pouvant être causés par les pierres, les engins de terrassement ou les outils à main, les rongeurs et les insectes, la corrosion chimique ou électrolytique, les effets des décharges atmosphériques, les phénomènes d'induction dus au voisinage de lignes d'énergie. Question 8/6

L.4 *Enveloppes de câble en aluminium*

Il est souhaitable de généraliser l'emploi de l'aluminium pour les enveloppes des câbles, pour autant que ces câbles ne soient pas plus chers que ceux à enveloppe en plomb et que les enveloppes en aluminium satisfassent mieux aux conditions techniques. L'utilisation de câbles à enveloppe en aluminium présente un intérêt particulier dans le cas des réseaux interurbains. Question 8/6

L.5 *Réalisation d'enveloppes de câble en métaux autres que le plomb ou l'aluminium*

D'autres types d'armures (par exemple avec de l'aluminium ondulé, des rubans en cuivre, etc.) peuvent être utilisés en fonction de l'application considérée. Question 8/6

L.7 *Application de la protection cathodique commune*

Par "protection cathodique commune de diverses structures métalliques souterraines", on entend une protection que l'on réalise contre la corrosion en utilisant des dispositifs protecteurs communs à ces structures. Un système de protection commun pour plusieurs structures métalliques souterraines comprend des liaisons électriques entre ces structures ainsi que des dispositifs protecteurs communs satisfaisant aux conditions de la protection et du drainage électrique cathodiques. Les méthodes de protection commune augmentent la fiabilité des structures enterrées, améliorent l'efficacité des dispositifs de protection cathodique et réduisent aussi le coût total ainsi que les frais d'entretien du système de protection. Question 7/6

L.16 *Matériaux plastiques conducteurs comme revêtements protecteurs des enveloppes métalliques de câbles*

Les avantages les plus importants de l'utilisation de câbles à revêtements CPM sont la protection coordonnée contre la corrosion, les coups de foudre et les effets électriques des lignes d'alimentation et de traction, la réduction du coût de la maintenance, particulièrement en ce qui concerne la mise à la terre, la simplification des projets de protection. Question 8/6

L.20 *Création d'un code de sécurité incendie pour les installations de télécommunication*

Tant pour les bâtiments existants que pour la conception et la construction de nouveaux bâtiments abritant des installations de télécommunication, chaque administration doit créer un code interne de sécurité incendie, en fonction de l'usage particulier auquel chaque bâtiment est destiné, contenant les directives minimales en matière de sécurité incendie et de protection contre le feu. Question 2/6

L.21 *Détection des incendies et systèmes d'alerte, détecteurs et sirènes d'alarme incendie*

Afin de protéger les biens et, le cas échéant, la vie, on peut installer des systèmes de protection par détection du feu et alarme qui rempliront un certain nombre de fonctions différentes telles que la détection et la localisation d'un feu, la fourniture d'une assistance pour confiner et/ou éteindre le feu, des procédures d'évacuation de secours, un appel aux services de lutte contre le feu. Question 2/6

L.22 *Protection incendie*

Compte tenu des dommages considérables que peuvent provoquer les incendies, ainsi que de l'importance de leur prévention en termes de sécurité, de fourniture de services et d'économie en systèmes de télécommunication, il est nécessaire de prendre en considération plusieurs aspects, tels que les suivants: réduction du coefficient de charge calorifique, cloisonnement du bâtiment en compartiments (secteurs de feu) afin de diminuer et de retarder la propagation du feu, statistiques d'incendies. Question 2/6

L.23 *Extinction des incendies – classification et répartition des installations et des équipements d'extinction dans les locaux*

Les moyens de lutte contre le feu à adopter dans un bâtiment de télécommunication peuvent varier selon l'usage, l'emplacement et le degré d'occupation des locaux: ce sont ces facteurs qui déterminent l'importance de l'assistance anti-incendie qui est initialement prévue en cas de sinistre. Question 2/6

L.25 *Maintenance des réseaux en câbles à fibres optiques*

Des systèmes de maintenance et des procédures permettent de surveiller la qualité d'un réseau à fibres optiques indépendamment de l'équipement de transmission. Question 5/6

L.28 *Protection externe additionnelle pour câbles terrestres marinisés*

Dans le cas des câbles pour eaux peu profondes, la probabilité de pannes est plus élevée que pour les applications en eaux profondes, en raison de phénomènes environnementaux (par exemple mouvement des vagues, séismes et glissements sous-marins, etc.) et en raison d'activités humaines affectant les fonds marins (par exemple la pêche, la pose et la maintenance d'autres câbles ou services).

En plus des diverses armures habituellement adoptées pour la construction des câbles (par exemple la superarmure (RA, *rocky armour*) telle que l'armure simple (SA, *single armour*) monocouche ou la double armure (DA, *double armour*) à deux couches), des protections externes additionnelles pourraient être adoptées en cas de besoin. De telles protections peuvent être mises en place aussi bien près des côtes en eaux peu profondes que dans la zone côtière comprise entre le bord de l'eau et la jonction littorale, ou le long du câble aux endroits où celui-ci risque d'être endommagé par des facteurs externes ou par la configuration des fonds marins. Question 10/6

L.32 *Dispositifs de protection des passages de câbles ménagés dans les séparations entre les secteurs de feu d'un bâtiment*

L'existence d'un grand nombre de passages de câbles dans les séparations entre les secteurs de feu d'un bâtiment de télécommunication diminue l'efficacité du système d'extinction. Une solution satisfaisante consiste à adopter des mesures passives de lutte contre la fumée et le feu, par exemple en étanchéifiant les passages de câbles à l'aide de matériaux ignifuges ou de systèmes de défense (protection) des câbles. Question 2/6

L.45 *Minimisation de l'incidence des installations extérieures de télécommunication sur l'environnement*

Cette Recommandation décrit dans le détail les méthodologies adoptées pour minimiser les effets de l'utilisation d'installations extérieures sur l'environnement (par exemple, en termes d'énergie et de dégagement de CO_2). Elle se fonde sur l'analyse du cycle de vie, c'est-à-dire de la possession du produit du "berceau jusqu'au tombeau". Question 1/6

L.46 *Protection des câbles et des installations de télécommunication contre les agressions biologiques*

Cette Recommandation décrit les types d'agressions biologiques que subissent les câbles de télécommunication et les mesures de protection associées. Elle traite des différents types d'agressions biologiques, des points faibles des câbles, des caractéristiques des dommages causés et envisage d'autres méthodes de protection des installations y compris en fonction de la position du câble.
Question 1/6

Les Recommandations suivantes contiennent des dispositions relatives à la disponibilité des réseaux SDH et OTN:

G.841 *Types et caractéristiques des architectures de protection des réseaux à hiérarchie numérique synchrone*

Cette Recommandation décrit les divers mécanismes de protection pour des réseaux en hiérarchie numérique synchrone (SDH) ainsi que leurs objectifs et leurs applications.

Les mécanismes de protection sont classés comme suit: protection d'un chemin SDH (au niveau de la section ou de la couche conduit) et protection d'une connexion de sous-réseau SDH (avec supervision intrinsèque, supervision sans intrusion et supervision de sous-couche). Questions Q.15, 16, 17, 18/15

G.842 *Interfonctionnement des architectures de protection des réseaux à hiérarchie numérique synchrone*

Cette Recommandation décrit les mécanismes d'interfonctionnement entre architectures de protection de réseau. L'interfonctionnement décrit ici s'applique à l'interconnexion à un nœud et à deux nœuds pour l'échange de trafic entre anneaux. Chaque anneau peut être configuré pour la protection partagée de section(s) de multiplexage ou pour la protection SNCP. Questions Q.15, 16, 17, 18/15

G.808.1 *Commutation générique de protection – Protection linéaire des chemins et des sous-réseaux*

Cette Recommandation donne un aperçu de la commutation de protection linéaire. Elle porte sur les systèmes de protection fondés sur les réseaux de transport optiques (OTN, *optical transport network*), sur les réseaux utilisant la hiérarchie numérique synchrone (SDH, *synchronous digital hierarchy*) et sur les réseaux utilisant le mode de transfert asynchrone (ATM, *asynchronous transfer mode*). L'aperçu des schémas de protection en anneau et de protection de sous-réseaux interconnectés (anneau par exemple) fera l'objet d'autres Recommandations. Questions Q.15, 16, 17, 18/15

G.873.1 *Réseau de transport optique: protection linéaire*

Cette Recommandation définit le protocole de commutateur de protection automatique (APS, *automatic protection switch*) et l'opération de commutation de protection pour les systèmes de protection linéaire du réseau de transport optique au niveau des unités de données de canal optique (ODUk, *optical channel data unit*). Les systèmes de protection examinés dans cette Recommandation sont les suivants: protection de chemin par unité ODUk; protection de connexion de sous-réseau par unité ODUk avec surveillance intrinsèque; protection de connexion de sous-réseau par unité ODUk avec surveillance non intrusive; protection de connexion de sous-réseau par unité ODUk avec surveillance de sous-couche. Questions Q.15, 16, 17, 18/15

G.781 *Fonctions des couches de synchronisation*

Fiabilité de la source de rythme SDH et PDH. Cette Recommandation spécifie une bibliothèque de modules de base, ainsi qu'un ensemble de règles de combinaison de ces modules pour décrire une fonctionnalité de synchronisation d'un équipement de transmission numérique.
Questions Q.15, 16, 17, 18/15

G.911 *Paramètres et méthodes de calcul de la fiabilité et de la disponibilité des systèmes à fibres optiques*

Fiabilité et disponibilité des systèmes à fibres optiques. Cette Recommandation définit un ensemble minimal de paramètres nécessaires pour décrire la fiabilité et la disponibilité des systèmes à fibres optiques, à savoir la fiabilité et la maintenance des systèmes, la fiabilité des dispositifs optiques actifs, la fiabilité des dispositifs optiques passifs ainsi que la fiabilité des fibres et câbles optiques. Cette Recommandation définit en outre des lignes directrices et des méthodes, accompagnées d'exemples, pour calculer la fiabilité prévue des dispositifs, ensembles et systèmes. Questions Q.15, 16, 17, 18/15

G.784 *Gestion de la hiérarchie numérique synchrone*

Gestion SDH. La Recommandation G.784 porte sur les fonctions de gestion des fautes, de la configuration, de la comptabilité, de la qualité et de la sécurité (FCAPS, *fault, configuration, accounting performance and security management*) des éléments de réseau SDH. Les aspects de gestion de la sécurité appellent un complément d'étude. Question Q.14/15

G.874 *Aspects gestion de l'élément de réseau optique de transport*

Gestion OTN. La Recommandation G.874 porte sur les fonctions de gestion des fautes, de la configuration, de la comptabilité, de la qualité et de la sécurité (FCAPS, *fault, configuration, accounting performance and security management*) des éléments de réseau OTN. Les aspects de gestion de la sécurité appellent un complément d'étude. Question Q.14/15

G.7712/Y.1703 *Architecture et spécification du réseau de communication de données*

Cette Recommandation inclut les aspects de sécurité des réseaux de communication de gestion (RCG) et des réseaux de communication de signalisation (RCS). Les fonctions de communications de données fournies dans cette Recommandation acceptent les services réseau en mode sans connexion. Il est possible que des versions futures de cette Recommandation comportent des fonctions additionnelles permettant d'accepter des services réseau en mode connexion. Question Q.14/15

Note: Il est possible que certaines Recommandations des séries G.650, 660 à 690, 950 à 970 contiennent des éléments liés à la fiabilité.

Annexe C: Liste des Commissions d'études et des Questions liées à la sécurité

Le travail de normalisation de l'UIT-T est effectué par les Commissions d'études (CE) techniques, au sein desquelles des représentants des membres de l'UIT-T élaborent des Recommandations (normes) dans les divers domaines des télécommunications internationales. Pour leurs travaux, les CE se fondent essentiellement sur des Questions mises à l'étude. Chacune de ces Questions porte sur des études techniques à réaliser dans un domaine particulier de la normalisation des télécommunications. Chaque CE a un président et un certain nombre de vice-présidents, désignés par l'Assemblée mondiale de normalisation des télécommunications (AMNT). On trouvera ci-après la liste des Commissions d'études de l'UIT-T pour la période d'études 2001-2004 avec leur titre, leur mandat et la liste des Questions à l'étude dans le domaine de la sécurité.

CE 2	Aspects opérationnels de la fourniture du service, réseaux et qualité de fonctionnement *Commission d'études directrice pour la définition des services, le numérotage et l'acheminement*
Mandat: Etudes se rapportant aux principes de fourniture du service, à la définition et aux critères opérationnels de l'émulation de service; aux prescriptions de numérotage, de nommage et d'adressage et à l'assignation des ressources, en particulier aux critères et procédures à suivre pour la réservation et l'assignation; aux prescriptions de routage et d'interfonctionnement; aux facteurs humains; aux aspects opérationnels des réseaux et aux critères de qualité de fonctionnement associés, en particulier la gestion du trafic du réseau, la qualité de service (ingénierie du trafic, qualité de fonctionnement opérationnelle et mesures en service); aux aspects opérationnels de l'interfonctionnement entre réseaux de télécommunication classiques et nouveaux réseaux; à l'évaluation des informations en retour des opérateurs, des équipementiers et des utilisateurs sur différents aspects de l'exploitation du réseau.	
Principales Questions liées à la sécurité: – Q.5/2 – Qualité de service des réseaux	

CE 3	Principes de tarification et de comptabilité et questions connexes de politique générale et d'économie des télécommunications
Mandat: Etudes se rapportant aux principes de tarification et de comptabilité pour les services internationaux de télécommunication et étude des questions connexes d'économie et de politique générale des télécommunications. A cette fin, la Commission d'études 3 encouragera en particulier la collaboration entre ses membres en vue de fixer des taux à des niveaux aussi bas que possible dans un souci d'efficacité du service et en tenant compte de la nécessité de conserver une gestion financière indépendante des télécommunications sur une base saine.	
Principales Questions liées à la sécurité: *Aucune*	

CE 4	Gestion des télécommunications, y compris le RGT *Commission d'études directrice pour le RGT*
Les études sur la sécurité menées par la CE 4 en tant que commission d'études directrice pour les activités de gestion concernent domaines suivants: a) considérations et spécifications relatives à l'architecture des interfaces de gestion; b) spécifications détaillées visant à sécuriser le réseau de gestion (également appelé plan de gestion), compte tenu notamment de la convergence actuelle des réseaux; c) protocole et modèles relatifs à la sécurisation des informations de gestion et à la gestion des paramètres de sécurité.	

La gestion du réseau de télécommunications est définie à différents niveaux d'abstraction, depuis la gestion des informations au niveau des éléments de réseau jusqu'aux services de gestion offerts au client. Les spécifications de sécurité pour les informations échangées entre systèmes de gestion ainsi qu'entre systèmes de gestion et éléments de réseau dépendent de la question de savoir si les réseaux de gestion relèvent d'une seule administration ou de plusieurs. Sur la base des principes architecturaux, des spécifications, mécanismes et protocoles explicites ont été définis dans des Recommandations existantes et d'autres sont en cours d'élaboration.

Principales Questions liées à la sécurité:
– Q.16/4 – Prise en charge de la gestion RGT pour les IMT-2000 et le réseau intelligent

CE 5	Protection contre les effets dus à l'environnement électromagnétique

La CE 5 est chargée des études se rapportant à la protection des réseaux et équipements de télécommunication contre les brouillages et la foudre ainsi que des études relatives à la compatibilité électromagnétique (CEM). Pour remplir sa mission, la CE 5 étudie plusieurs Questions et élabore des Recommandations et Manuels permettant de contribuer à la sécurité du réseau contre les menaces électromagnétiques (par exemple les phénomènes malveillants d'origine humaine de transitoires à puissance élevée tels que les impulsions électromagnétiques à haute altitude (HEMP, *high-altitude electromagnetic pulse*) et les hyperfréquences à puissance élevée (HPM, *high-power microwave*). Dans le cadre de la sécurité électromagnétique, on s'intéresse également aux fuites d'informations des réseaux de télécommunication dues aux rayonnements imprévus des équipements.

La nature des menaces malveillantes et les techniques d'atténuation correspondantes sont analogues à celles qui s'appliquent aux perturbations électromagnétiques naturelles ou non intentionnelles. Les activités traditionnelles de la Commission d'études 5 relatives à la protection contre la foudre et au contrôle des brouillages électromagnétiques contribuent donc à la sécurité du réseau contre les menaces malveillantes d'origine humaine. La CE 5 est actuellement chargée de l'étude de six Questions se rapportant à la sécurité électromagnétique du réseau de télécommunication.

Les menaces électromagnétiques malveillantes d'origine humaine et les perturbations électromagnétiques naturelles ou non intentionnelles présentent de nombreuses analogies mais aussi des différences de taille. Pour remplir sa mission, la CE 5 étudie plusieurs Questions et élabore des Recommandations et des Manuels permettant de contribuer à la sécurité du réseau contre les menaces électromagnétiques.

Dans le cadre de la sécurité électromagnétique, on s'intéresse essentiellement aux deux points suivants:

- Résistance et immunité des réseaux et équipements de télécommunication aux phénomènes malveillants d'origine humaine de transitoires à puissance élevée, provenant notamment:
  - des champs électromagnétiques produits par des explosions nucléaires à haute altitude – impulsions électromagnétiques à haute altitude (HEMP, *high-altitude electromagnetic pulse*).
  - des générateurs électromagnétiques à puissance élevée (HPE, *high-power electromagnetic*), y compris les sources d'hyperfréquences à puissance élevée (HPM, *high-power microwave*) et les sources à ultra large bande (UWB, *ultra-wideband*).
- Risque de fuites d'informations des réseaux de télécommunication dues aux rayonnements imprévus des équipements.

La prise de conscience des menaces de sécurité liées à ces phénomènes s'est récemment accrue du fait de leur vulgarisation par le biais d'articles, de reportages et de programmes télévisés.

La nature des menaces électromagnétiques malveillantes et les techniques d'atténuation correspondantes sont analogues à celles qui s'appliquent aux perturbations électromagnétiques naturelles ou non intentionnelles. Il existe par exemple des analogies entre les impulsions HEMP et les impulsions électromagnétiques créées par la foudre. Les techniques d'occultation et de filtrage qui permettent aux équipements de réduire leurs rayonnements non désirés permettent aussi de réduire le risque de fuite d'énergie non intentionnelle. Les activités traditionnelles de la Commission d'études 5 relatives à la protection contre la foudre et au contrôle des brouillages électromagnétiques contribuent donc à la sécurité du réseau contre les menaces malveillantes d'origine humaine. Les Questions suivantes, dont l'étude a été confiée à la Commission d'études 5 pendant la période d'études 2001-2004, se rapportent à la sécurité du réseau.

Principales Questions liées à la sécurité:

– Q.2/5 – Compatibilité électromagnétique dans les systèmes d'accès large bande (*Le contrôle des rayonnements non désirés des systèmes d'accès à large bande contribue à réduire le risque de fuites d'informations).*

– Q.4/5 – Résistance de nouveaux types d'équipement de télécommunication et de réseau d'accès (*La résistance des équipements à la foudre permet d'améliorer la résistance des équipements aux surtensions induites par les impulsions HEMP*).

– Q.5/5 – Protection contre la foudre des systèmes fixes, mobiles et sans fils (*Les techniques utilisées pour la protection contre la foudre permettent également de renforcer la protection des équipements contre les impulsions HEMP et les rayonnements HPE*).

– Q.6/5 – Configurations d'équipotentialité et mise à la terre des systèmes de télécommunication dans l'environnement mondial (*Des mesures appropriées relatives à l'équipotentialité et à la mise à la Terre permettent également de renforcer la protection des équipements contre les impulsions HEMP et les rayonnements HPE*).

– Q.12/5 – Mise à jour et amélioration des Recommandations existantes relatives à la compatibilité électromagnétique (*La compatibilité électromagnétique des équipements de télécommunication améliore leur immunité aux impulsions HEMP conduites et rayonnées ainsi qu'aux rayonnements HPE. Elle réduit par ailleurs le risque de fuites d'informations*).

– Q.13/5 – Mise à jour et amélioration des Recommandations existantes relatives à la résistance (*La résistance des équipements à la foudre améliore leur résistance aux surtensions induites par les impulsions HEMP*).

CE 6	Installations extérieures

Mandat: Etudes se rapportant aux installations extérieures telles que: construction, installation, raccordement, terminaison et protection contre la corrosion et les autres formes de dommages causés par l'environnement, à l'exception des phénomènes électromagnétiques, de tous les types de câble pour les télécommunications publiques et des structures associées.

Principales Questions liées à la sécurité:

– Q.1/6 – Problèmes environnementaux dans les installations de télécommunication

– Q. 2/6 – Protection des installations de télécommunication contre les incendies

– Q. 5/6 – Maintenance des réseaux de câbles optiques

CE 9	Réseaux en câble intégrés à large bande et transmission télévisuelle et sonore *Commission d'études directrice pour les réseaux de télévision et câblés intégrés large bande.*

La Commission d'études de l'UIT-T chargée des "Réseaux en câble intégrés à large bande et transmission télévisuelle et sonore" (CE 9) est la Commission d'études directrice pour les réseaux de télévision et câblés intégrés large bande. Elle élabore et tient à jour les Recommandations portant sur:

- l'utilisation des réseaux en câble et des réseaux hybrides conçus avant tout pour la distribution chez le particulier de programmes de télévision et de programmes radiophoniques, par exemple réseaux intégrés à large bande pour acheminer les services vocaux et d'autres services à paramètre temps critique, la vidéo à la demande et les services interactifs, etc.;
- l'utilisation des systèmes de télécommunication pour la contribution, la distribution primaire et la distribution secondaire de programmes de télévision, de programmes radiophoniques et de services de données similaires.

Dans le cadre de sa mission, la CE 9 évalue les menaces et les vulnérabilités relatives aux réseaux et services à large bande, définit des objectifs en termes de sécurité, évalue les contre-mesures et définit des architectures de sécurité. En termes de sécurité, elle s'intéresse essentiellement aux services de sécurisation de l'accès large bande, aux services de sécurisation de la téléphonie IP, aux services de sécurisation des connexions de réseau domestiques et aux environnements applicatifs sécurisés pour les services de télévision interactive.

Les activités relatives à la sécurité portent essentiellement sur:

- *Les services de sécurisation de l'accès large bande:* services de sécurité pour les réseaux d'accès à large bande, à savoir authentification du câblomodem, gestion des clés de chiffrement, confidentialité et intégrité des données transmises et téléchargement sécurisé de logiciels de câblomodem.
- *Les services de sécurisation de la téléphonie IP:* IPCablecom est un projet spécial sur la fourniture de services interactifs à temps critique sur le réseau de transmission de télévision par câble au moyen du protocole IP, en particulier la voix et la vidéo sur IP. Les services de sécurité offerts dans le réseau IPCablecom comprennent l'authentification de l'adaptateur de terminal multimédia (MTA, *multimedia terminal adapter*) auprès du fournisseur de services, l'authentification du fournisseur de services auprès de l'adaptateur MTA, la fourniture et la configuration sécurisées des dispositifs, la gestion sécurisée des dispositifs, la transmission sécurisée de la signalisation et la transmission sécurisée des médias.
- *Les services de sécurisation des connexions de réseau domestiques:* des câblomodems améliorés peuvent offrir des services de réseau domestique tels que des pare-feu ou la traduction d'adresse de réseau. Les services de sécurité prévus pour les câblomodems améliorés comprennent l'authentification de l'adaptateur de terminal multimédia (MTA, *multimedia terminal adapter*) auprès du fournisseur de services, l'authentification du fournisseur de services auprès de l'adaptateur MTA, la fourniture et la configuration sécurisée des dispositifs, la gestion sécurisée des dispositifs, la fonctionnalité de pare-feu/filtrage de paquets, la gestion sécurisée des pare-feu et le téléchargement sécurisé de logiciels de câblomodems améliorés.
- *Les environnements applicatifs sécurisés pour les services de télévision interactive:* les services de télévision interactive s'appuient sur les services de sécurité définis en Java et sur la spécification de la plate-forme domestique multimédia (MHP, *multimedia home platform*).

Principales Questions liées à la sécurité:
– Q.6/9 – Accès conditionnel et protection antipiratage dans la télévision numérique directe par câble
– Q13/9 – Applications vocales et vidéo de type IP sur réseaux de télévision par câble

CE 11	Spécifications et protocoles de signalisation *Commission d'études directrice pour les réseaux intelligents*

Mandat: Etudes se rapportant aux spécifications et protocoles de signalisation pour les fonctions utilisant le protocole Internet (IP), certaines fonctions liées à la mobilité, les fonctions multimédias, et améliorations des Recommandations existantes sur les protocoles d'accès et les protocoles de signalisation interréseau des réseaux ATM, du RNIS à bande étroite et du RTPC.

Principales Questions liées à la sécurité:

– Q.1/11 – Prescriptions de signalisation pour la prise en charge des nouveaux services à valeur ajoutée de type IP et RI

– Q.6/11 – Prescriptions de signalisation pour l'interfonctionnement des services sur les réseaux d'accès à l'Internet par le réseau commuté et les réseaux de communication vocale, de données et multimédia de type IP

– Q.12/11 – Signalisation d'accès et de réseau pour les services évolués à bande étroite et à large bande

CE 12	Qualité de transmission de bout en bout des réseaux et terminaux *Commission d'études directrice pour la qualité de service et de fonctionnement*

Mandat: Etudes se rapportant à la qualité de transmission de bout en bout des réseaux et terminaux par rapport à la qualité perçue et à l'acceptabilité par l'utilisateur des signaux de texte, de paroles et d'images ainsi qu'aux incidences correspondantes sur la transmission de tous les réseaux (par exemple, ceux utilisant les systèmes PDH, SDH, ATM et IP) et de tous les terminaux de télécommunication (par exemple, combiné, mains-libres, casque, téléphone mobile, système audiovisuel et réponse vocale interactive).

Principales Questions liées à la sécurité:

– Q.12/12 – Considérations relatives à la qualité de transmission des services en bande vocale sur les réseaux utilisant le protocole Internet (IP)

– Q.13/12 – Exigences de QoS/performances pour les systèmes multimédias

CE 13	Réseaux multiprotocoles et réseaux utilisant le protocole IP et leur interréseautage *Commission d'études directrice pour les questions relatives au protocole IP, le RNIS à large bande, l'infrastructure mondiale de l'information et les questions relatives aux satellites*

Mandat: Etudes se rapportant:

- à l'interréseautage de réseaux hétérogènes mettant en œuvre plusieurs domaines;
- aux multiples protocoles et aux technologies novatrices permettant de réaliser un réseautage fiable et de haute qualité;
- aux aspects particuliers que sont l'architecture, l'interfonctionnement et l'adaptation, la qualité de bout en bout, le routage et les spécifications de transport.

En tant que Commission d'études directrice pour les questions relatives au protocole IP, le RNIS à large bande, l'infrastructure mondiale de l'information et les questions relatives aux satellites ainsi que le nouveau projet NGN, elle traite d'un grand nombre de problèmes de sécurité dans des domaines très divers.

Traditionnellement, la Commission d'études 13 de l'UIT-T aborde implicitement des aspects de sécurité lorsqu'elle étudie l'architecture et la structure de réseau, sachant qu'il est absolument nécessaire de traiter ces aspects (du point de vue de l'architecture et de l'implémentation) afin qu'un réseau puisse être fonctionnel et fiable.

Les difficultés rencontrées avec les aspects de sécurité augmentent lorsqu'on met en œuvre les nouvelles techniques numériques de commutation par paquet – plus ou moins ouvertes – et l'environnement libéralisé, décrit par exemple dans le cadre de l'infrastructure GII. Ceci est particulièrement vrai lorsque des tiers interviennent dans la "chaîne de valeurs ajoutées" associée à l'infrastructure GII (ou à un réseau NGN, sous-ensemble de cette infrastructure). Dans cet environnement, le problème de la sécurité avec toutes ses facettes sera encore plus important et doit être traité de manière explicite.

La Commission d'études 13 a donc décidé d'incorporer dans chaque Recommandation nouvelle ou révisée un paragraphe sur la sécurité afin de faire référence aux paragraphes de la Recommandation qui traitent d'aspects de sécurité. Même si aucun aspect de sécurité n'est traité dans une Recommandation, il convient de le mentionner dans ce paragraphe spécial sur la sécurité. La CE 17 a décidé à son tour de procéder à cette incorporation et a invité toutes les Commissions d'études de l'UIT-T à faire de même.

La CE 13 a par ailleurs décidé que les Recommandations contenant des spécifications relatives à la sécurité soient signalées à la CE 17 afin que celle-ci puisse mettre à jour rapidement le "catalogue des Recommandations approuvées incluant des aspects de sécurité" et le "recueil des définitions relatives à la sécurité approuvées par l'UIT-T".

Le nouveau projet NGN porte sur des aspects de sécurité dans plusieurs paragraphes, notamment au § 6.6.

Principales Questions liées à la sécurité:

– Q.1/13 – Principes, prescriptions, cadres structurels et architectures d'un environnement général de réseau hétérogène
– Q.3/13 – Exploitation, maintenance et gestion des réseaux à protocole Internet (IP) et autres réseaux
– Q.4/13 – Gestion des ressources large bande et IP
– Q.6/13 – Qualité de fonctionnement des réseaux IP dans la nouvelle infrastructure mondiale de l'information
– Q.7/13 – Transfert de cellules ATM/RNIS-B et disponibilité
– Q.8/13 – Qualité de fonctionnement rapportée aux erreurs de transmission et à la disponibilité
– Q.10/13 – Architecture et principes d'interfonctionnement des réseaux centraux
– Q.11/13 – Mécanismes permettant à des services IP utilisant la MPLS de fonctionner dans le réseau public

CE 15	Réseaux optiques et autres réseaux de transport *Commission d'études directrice pour le transport dans le réseau d'accès et pour les technologies optiques*

La Question 14 de la CE 15 (Q.14/15) porte sur la spécification des prescriptions de gestion et de contrôle et sur la prise en charge de modèles d'information pour les équipements de transport. Elle s'appuie sur le concept de RGT et sur le cadre du RGT établis par l'UIT-T pour la définition de ces prescriptions et de ces modèles. La gestion de la sécurité, qui correspond à l'une des cinq catégories fonctionnelles essentielles de gestion du RGT, est étudiée dans le cadre de la Question 14/15.

- Prescriptions de gestion des équipements de transport: les Recommandations G.7710/Y.1701, G.784 et G.874 portent sur les fonctions de gestion d'équipement (EMF, *equipment management function*) qui sont contenues dans un élément de réseau de transport et qui sont respectivement communes à plusieurs techniques, propres aux éléments de réseau SDH et propres aux éléments de réseau OTN. Des applications sont décrites pour la date et l'heure, la gestion des fautes, la gestion de la configuration, la gestion de la comptabilité, la gestion de la qualité et la gestion de la sécurité. Ces applications conduisent à la spécification des fonctions EMF et de leurs prescriptions. Les prescriptions de gestion de la sécurité dans ces Recommandations sont actuellement à l'étude.

- Architecture et spécification du réseau de communication de données: la Recommandation G.7712/Y.1703 définit les exigences d'architecture pour un réseau de communication de données (RCD) qui peut accepter les communications de gestion répartie se rapportant au réseau de gestion des télécommunications (RGT), les communications de signalisation répartie se rapportant au réseau de transport à commutation automatique (ASTN) et les autres communications réparties (par exemple, communications de service ou vocales, téléimportation de logiciel). Diverses applications (par exemple, RGT, ASTN, etc.) nécessitent un réseau de communication par paquets afin de transporter les informations entre les différents composants. Par exemple, le RGT a besoin d'un réseau de communication, appelé *réseau de communication de gestion* (RCG) pour transporter les messages de gestion entre les composants du RGT (par exemple, le composant NEF et le composant OSF). L'ASTN a besoin d'un réseau de communication, appelé *réseau de communication de signalisation* (RCS) pour transporter les messages de signalisation entre les composants de l'ASTN (par exemple, les composants CC). La Recommandation G.7712/Y.1703 fait référence à la Recommandation M.3016 concernant les prescriptions de sécurité du réseau RCG. Les prescriptions de sécurité du réseau RCS sont définies dans la Recommandation G.7712/Y.1703.
- Gestion répartie des appels et des connexions: la Recommandation G.7713/Y.1704 spécifie la gestion répartie des appels et des connexions à l'interface utilisateur-réseau (UNI, *user network interface*) et à l'interface de nœud de réseau (NNI, *network node interface*). Elle spécifie plus particulièrement les communications aux interfaces permettant d'effectuer automatiquement les opérations relatives aux appels et aux connexions. Elle spécifie des attributs, notamment des attributs de sécurité permettant de vérifier les opérations relatives aux appels et aux connexions (par exemple une information permettant d'authentifier la demande d'appel et éventuellement de contrôler l'intégrité de cette demande d'appel).
- Architecture et prescriptions de routage dans les réseaux optiques à commutation automatique: la Recommandation G.7715/Y.1706 définit les prescriptions et l'architecture pour les fonctions de routage utilisées pour l'établissement des connexions commutées (SC, *switched connection*) et des connexions permanentes logicielles (SPC, *soft permanent connection*) dans le cadre du réseau optique à commutation automatique (ASON, *automatically switched optical network*). Parmi les principaux aspects traités dans cette Recommandation, figurent l'architecture de routage ASON et les composants fonctionnels, notamment le choix du chemin, les attributs de routage, les messages abstraits et les diagrammes d'état. Cette Recommandation fait référence aux Rec. UIT-T M.3016 et X.800 concernant les aspects de sécurité. Elle précise notamment que, en fonction des conditions d'utilisation d'un protocole de routage, les objectifs généraux de sécurité définis dans la Recommandation UIT-T M.3016 en matière de confidentialité, d'intégrité des données, de responsabilité et de disponibilité peuvent revêtir différents niveaux d'importance. Pour procéder à une analyse des menaces concernant un protocole de routage envisagé, il faut tenir compte des aspects suivants en s'appuyant sur la Rec. UIT-T X.800: usurpation d'identité, écoute clandestine, accès non autorisé, perte ou altération d'informations (notamment attaque par réexécution), répudiation, fabrication et déni de service.
- Cadre de gestion du réseau ASON: la Recommandation G.fame porte sur les aspects de gestion du plan de commande ASON et sur les interactions entre le plan de gestion et le plan de commande ASON. Des prescriptions relatives à la gestion des fautes, à la gestion de la configuration, à la gestion de la comptabilité, à la gestion de la qualité et à la gestion de la sécurité pour les composants du plan de commande seront incluses.

Principales Questions liées à la sécurité:
– Q.14/15 – Gestion de réseau pour systèmes et équipements de transport

CE 16	Services, systèmes et terminaux multimédias *Commission d'études directrice pour les services, systèmes et terminaux multimédias et pour les affaires électroniques et le commerce électronique*

La Commission d'études 16 est la Commission d'études directrice pour les services, systèmes et terminaux multimédias ainsi que pour les affaires électroniques et le commerce électronique. La Question G (confiée au GT 2/16), intitulée "Sécurité des systèmes et services multimédias", porte sur les problèmes de sécurité suivants.

Les applications multimédias avancées (par exemple la téléphonie sur réseaux par paquets, la téléphonie IP, les services interactifs de conférence et de collaboration; la messagerie multimédia, la transmission audio/vidéo en continu, etc.) sont soumises à diverses menaces de sécurité cruciales dans les environnements hétérogènes. Les mauvaises utilisations, les modifications malveillantes, l'écoute indiscrète et les attaques de type déni de service ne sont que des exemples de risques potentiels, notamment sur les réseaux IP.

Il est admis que ces applications ont des besoins de sécurité communs qui peuvent être satisfaits par des mesures de sécurité génériques, par exemple par une sécurité au niveau du réseau. Néanmoins, les applications multimédias ont généralement des besoins de sécurité qui leur sont propres et pour lesquels le mieux est de prévoir des mesures de sécurité au niveau de la couche application. Dans le cadre de la Question G, on s'intéresse essentiellement aux problèmes de sécurité des applications multimédias au niveau de la couche application et on tient compte de moyens de sécurité complémentaires au niveau du réseau si besoin est.

Principales Questions liées à la sécurité:
– Q.G/16 – Sécurité des systèmes et services multimédias

CE 17	Réseaux de données et logiciels de télécommunication *Commission d'études directrice pour le relais de trames, pour la sécurité des systèmes de communication et pour les langages et les techniques de description*

Mandat: Etudes se rapportant aux réseaux de communication de données et à l'application des communications entre systèmes ouverts y compris le réseautage, l'annuaire et la sécurité, et aux langages techniques, à leur méthode d'utilisation et à d'autres problèmes connexes liés aux aspects logiciels des systèmes de télécommunication.

Principales Questions liées à la sécurité:
– Q.9/17 – Services et systèmes d'annuaire
– Q.10/17 – Prescriptions de sécurité, modèles et lignes directrices pour les systèmes et services de communication (Note – la Commission d'études 17 a décidé de subdiviser la Question 10/17 en 6 Questions distinctes: G/17 – Projet de sécurité; H/17 – Architecture et cadre de sécurité; I/17 – Cybersécurité; J/17 – Gestion de la sécurité; K/17 – Télébiométrie; et L/17 – Services de communication sécurisés)

CES	Commission d'études spéciale "IMT-2000 et systèmes ultérieurs" *Commission d'études directrice pour les IMT-2000 et les systèmes ultérieurs et pour la mobilité*
La Commission d'études spéciales de l'UIT-T sur les IMT-2000 et les systèmes ultérieurs inclut la sécurité parmi les aspects fondamentaux de ses Recommandations faisant référence aux membres de la famille des IMT-2000 (3G) identifiés dans ses Recommandations des séries Q.1741.x (3GPP) et Q.1742.x (3GPP2). Ces Recommandations portent notamment sur une évaluation des menaces perçues et sur une liste de prescriptions de sécurité pour faire face à ces menaces, sur des objectifs et des principes de sécurité, sur une architecture de sécurité définie (c'est-à-dire des éléments et des mécanismes de sécurité), sur des spécifications relatives aux algorithmes de chiffrement ainsi que sur des prescriptions, une architecture et des fonctions concernant les interceptions licites. Les études sont réalisées dans le cadre des Questions 3, 6 et 7/CES. Les études relatives aux interceptions licites visent essentiellement à déterminer les interceptions utiles ainsi que les informations liées à la surveillance que les fournisseurs de services doivent fournir aux services nationaux chargés de faire respecter la loi. Les informations relatives aux interceptions et le contenu des communications peuvent dépendre ou non du type de réseau mobile 3G ou 3G amélioré.	
Principales Questions liées à la sécurité: – 3/CES – Identification des systèmes IMT-2000 existants ou en évolution – 6/CES – Harmonisation des systèmes IMT-2000 en évolution – 7/CES – Convergence des systèmes fixes et des systèmes IMT-2000 existants	

Modules de sécurité de l'UIT-T

Cadre de l'architecture de sécurité

X.800 – Architecture de sécurité
X.802 – Modèle de sécurité pour les couches inférieures
X.803 – Modèle de sécurité pour les couches supérieures
X.805 – Architecture de sécurité pour les systèmes assurant des communications de bout en bout
X.810 – Cadres de sécurité pour les systèmes ouverts: aperçu général
X.811 – Cadres de sécurité pour les systèmes ouverts: cadre d'authentification
X.812 – Cadres de sécurité pour les systèmes ouverts: cadre de contrôle d'accès
X.813 – Cadres de sécurité pour les systèmes ouverts: cadre de non-répudiation
X.814 – Cadres de sécurité pour les systèmes ouverts: cadre de confidentialité
X.815 – Cadres de sécurité pour les systèmes ouverts: cadre d'intégrité
X.816 – Cadres de sécurité pour les systèmes ouverts: cadre d'audit et d'alarmes de sécurité

Protocoles

X.273 – Protocole de sécurité de la couche réseau
X.274 – Protocole de sécurité de la couche transport

Sécurité en mode relais de trame

X.272 – Compression et secret des données dans les réseaux à relais de trames

Techniques de sécurité

X.841 – Objets d'information de sécurité pour le contrôle d'accès
X.842 – Lignes directrices pour l'utilisation et la gestion des services de tiers de confiance
X.843 – Spécification des services utilisant des tierces parties de confiance pour autoriser l'emploi de signatures numériques

Services d'annuaire et authentication

X.500 – Aperçu général des certificats de clé publique et d'attribut
X.501 – Les Modèles
X.509 – Cadre général des certificats de clé publique et d'attribut
X.519 – Spécification du protocole

Sécurité de gestion de réseau

M.3010 – Principes des réseaux de gestion des télécommunications
M.3016 – Aperçu général de la sécurité du RGT
M.3210.1 – Services de gestion RGT pour la gestion de la sécurité des réseaux IMT-2000
M.3320 – Cadre général des prescriptions de gestion pour l'interface X du réseau de gestion des télécommunications
M.3400 – Fonctions de gestion RGT

Gestion des systèmes

X.733 – Fonction de signalisation des alarmes
X.735 – Fonction de commande des registres de consignation
X.736 – Fonction de signalisation des alarmes de sécurité
X.740 – Fonction de piste de vérification de sécurité
X.741 – Objets et attributs pour le contrôle d'accès

Télécopie

T.30 Annexe G – Procédures pour la transmission sécurisée de documents de télécopie du Groupe 3 utilisant les systèmes HKM et HFX
T.30 Annexe H – Sécurisation de la télécopie G3 sur la bse de l'algorithme RSA
T.36 – Capacités de sécurité à utiliser avec les télécopieurs du Groupe 3
T.503 – Profil d'application de document pour l'échange de documents de télécopie du Groupe 4
T.563 – Caractéristiques des télécopieurs du Groupe 4

Systèmes de télévision et systèmes de transmission par câble

J.91 – M'éthodes techniques pour garantir la confidentialité sur les transmissions internationales de télévision à grande distance
J.93 – Prescriptions d'accès conditionnel dans le réseau de distribution secondaire de la télévision numérique par câble
J.170 – Spécification de la sécurité sur IPCablecom

Communications multimédias

H.233 – Système de confidentialité pour les services audiovisues
H.234 – Système de gestion de clés de chiffrement et d'authentification pour les services audiovisuels
H.235 – Sécurité et chiffrement pour les terminaux multimédias de la série H (terminaux H.323 et autres terminaux de type H.245)
H.323 Annexe J – Systèmes de communication multimédia en mode paquet – Sécurisation des dispositifs de l'Annexe F/H.323 (Sécurisation des dispositifs d'extrémité simples)
H.350.2 – Architecture des services d'annuaire pour les protocoles H.325
H.530 – Procédures de sécurité symétrique pour la mobilité des systèmes H.323 selon la Recommandation H.510

Les Recommandations de l'UIT-T sont accessibles sur le site web de l'UIT à l'adresse http://www.itu.int/publications/bookshop/how-to-buy.html (on trouvera également sur cette page des informations concernant l'accès gratuit à un nombre limité de Recommandations de l'UIT)

Les sujets importants que l'UIT-T traite actuellement du point de vue de la sécurité sont les suivants:

Télébiometrie, gestion de la sécurité, sécurité de la mobilité, telecommunications d'urgence

Pour plus d'informations sur l'UIT-T et sur ses Commissions d'études, on se reportera à l'adresse: http://www.itu.int/ITU-T