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

UIT-T

Secteur de la normalisation des télécommunications de l'UIT

2012

UIT-T

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

Janvier 2012

Préface

Malcolm Johnson
Directeur
Bureau de la normalisation des télécommunications de l'UIT

Il y a encore relativement peu, la sécurité des technologies de l'information et de la communication (TIC) concernait principalement des domaines d'application tels que les transactions bancaires, l'aérospatial et la défense. Toutefois, avec la croissance rapide et généralisée de l'utilisation des communications de données et, en particulier, de l'Internet, la sécurité est à présent l'affaire de tous.

L'ampleur prise par la sécurité des TIC peut être attribuée en partie à des incidents qui ont défrayé la chronique tels que des virus, des piratages et des menaces d'atteinte à la vie privée. Mais la réalité est que les ordinateurs et les réseaux font désormais tellement partie de la vie quotidienne, qu'il est maintenant impératif de mettre en place des mesures de sécurité efficaces afin de protéger les systèmes TIC des pouvoirs publics, de l'industrie, du commerce, des infrastructures critiques et des particuliers. Par ailleurs, de nombreux pays disposent à présent d'une législation sur la protection des données exigeant le respect de normes de protection reconnues.

Pour être vraiment efficace, la sécurité doit être prise en compte à toutes les étapes du cycle de vie des systèmes, depuis leur définition et leur conception jusqu'à leur mise hors service, en passant par leur mise en œuvre et leur déploiement. Le fait de ne pas tenir suffisamment compte de la sécurité au cours d'une de ces étapes peut avoir pour conséquence de mettre en péril les systèmes ou les données. Les organismes de normalisation ont un rôle essentiel à jouer en faisant en sorte que les enjeux liés à la sécurité des TIC soient mieux connus et que les considérations relatives à la sécurité constituent une partie fondamentale des spécifications, et en fournissant des normes techniques et des indications aux personnes chargées de la mise en œuvre et aux utilisateurs, afin de les aider à rendre les systèmes et les services de communication suffisamment robustes pour résister aux cyberattaques.

L'UIT-T joue depuis longtemps un rôle actif dans les travaux relatifs à la sécurité des TIC, mais a vu dernièrement l'ampleur de sa tâche augmenter de manière considérable, en raison de l'apparition de nouvelles menaces et de l'évolution des menaces existantes, ainsi que des demandes de nos membres, qui ont besoin de normes pour les aider à contrer ces menaces. Le présent Manuel expose certains aspects essentiels de ces travaux et présente les nombreuses ressources que l'UIT-T met à la disposition des utilisateurs pour les aider à traiter les problèmes liés à la sécurité des TIC auxquels nous sommes confrontés.

La normalisation joue un rôle essentiel dans l'instauration d'une culture mondiale de la cybersécurité. Nous pouvons remporter la lutte contre les cybermenaces et nous le ferons, en nous appuyant sur les travaux accomplis par les milliers d'individus engagés qui, issus des administrations publiques, du secteur privé et des établissements universitaires, se rassemblent dans des organisations comme l'UIT pour élaborer des normes relatives à la sécurité et des lignes directrices sur les bonnes pratiques. Ces travaux ne sont ni fascinants, ni très en vue, mais ils n'en sont pas moins essentiels à la sauvegarde de notre avenir numérique. Je tiens à exprimer toute ma gratitude aux ingénieurs du Bureau de la normalisation des télécommunications de l'UIT qui, conjointement avec des experts provenant d'Etats Membres de l'UIT, ont travaillé et continuent de travailler inlassablement à l'élaboration de ces normes et de ces lignes directrices.

J'espère que le présent Manuel vous permettra de mieux comprendre les questions relatives à la sécurité des TIC et les travaux menés par l'UIT-T dans ce domaine, et j'invite les lecteurs à me communiquer leurs réactions en vue des prochaines éditions.

Malcolm Johnson

Directeur
Bureau de la normalisation des télécommunications, UIT

Remerciements

Le présent Manuel est le résultat des contributions de nombreux auteurs, qui ont participé à l'élaboration des Recommandations UIT-T pertinentes, ou qui ont pris part à des réunions de Commissions d'études, à des ateliers ou à des séminaires de l'UIT-T. Il convient de féliciter les Rapporteurs, les éditeurs et les coordonnateurs sur la sécurité des Commissions d'études de l'UIT, ainsi que Martin Euchner, Conseiller de la Commission d'études 17, et son prédécesseur Georges Sebek, et, en particulier, Herb Bertine, ancien Président de la Commission d'études directrice de l'UIT-T pour les travaux sur la sécurité des télécommunications, et Mike Harrop, ancien Rapporteur pour le projet relatif à la sécurité et rédacteur en chef du présent Manuel.

Résumé analytique

Le présent Manuel consiste en un exposé général sur les travaux de l'UIT-T dans le domaine de la sécurité des TIC et, plus précisément, vise à résumer la manière dont l'UIT-T lutte contre les menaces qui pèsent sur la cybersécurité mondiale, en élaborant des Recommandations et des documents d'orientation et en menant des initiatives de sensibilisation. Il est destiné en premier lieu aux personnes s'occupant de la sécurité des informations et des communications et des normes associées, ou à celles pour qui ce domaine et les normes qui s'y rattachent présentent un intérêt, et s'adresse également aux personnes qui ont simplement besoin de mieux comprendre les questions relatives à la sécurité des TIC.

L'ouvrage peut être utilisé de différentes façons suivant l'organisation, le rôle et les besoins du lecteur. Les chapitres d'introduction fournissent un aperçu des principaux domaines sur lesquels portent les travaux actuels de l'UIT-T en matière de sécurité et donnent lieu à une étude des exigences de base pour la protection des applications et des services TIC et la sécurité des informations. Outre la présentation des menaces et des vulnérabilités sur lesquelles se fondent les exigences de sécurité et l'étude du rôle joué par les normes pour se conformer à ces exigences, il est question de certains éléments nécessaires à la protection des diverses entités qui fournissent ou utilisent des technologies et des services d'information et de communication, ou qui jouent un rôle d'appui pour ces technologies et ces services. Enfin, on trouve en ce début d'ouvrage des explications concernant l'importance des normes relatives à la sécurité des TIC et des exemples illustrant la manière dont les travaux de l'UIT-T relatifs à la sécurité évoluent en vue de satisfaire aux exigences en matière de sécurité.

S'ensuit une présentation des architectures de sécurité génériques pour les systèmes ouverts et les communications de bout en bout, accompagnée d'exemples d'architectures propres à certaines applications. Chacune de ces architectures établit un cadre dans lequel les multiples aspects de la sécurité peuvent s'appliquer de manière cohérente. Elles permettent également de normaliser les concepts qui servent de fondements aux services et aux mécanismes de sécurité, et contribuent à établir un lexique normalisé pour les termes et les concepts fondamentaux du domaine de la sécurité des TIC. Les principes généraux énoncés dans le cadre de ces architectures servent de base à de nombreuses autres normes relatives à des services, des mécanismes et des protocoles de sécurité, normes dont certaines sont étudiées dans la suite de l'ouvrage.

La gestion de la sécurité regroupe de nombreuses activités liées au contrôle et à la protection de l'accès aux ressources de système et de réseau, à la surveillance et à la signalisation des événements, aux politiques et aux audits, ainsi qu'à la gestion des informations relatives à ces fonctions et activités. Un chapitre du manuel est consacré à la gestion de la sécurité des informations, à la gestion des risques et à la gestion des actifs. Vient ensuite l'étude des activités de gestion relatives à la sécurisation de l'infrastructure de réseau, dans un chapitre portant sur la nécessité de sécuriser les données utilisées pour la surveillance et le contrôle du réseau de télécommunication, ainsi que sur des questions relatives à la gestion du réseau et aux services usuels de gestion de la sécurité.

Le manuel traite également du rôle d'appui joué par l'annuaire dans l'authentification et dans le fonctionnement d'autres services de sécurité, et décrit les principaux domaines qui dépendent des services d'annuaire, à savoir la gestion d'identité, les infrastructures de clé publique, la télébiométrie (c'est-à-dire l'identification et l'authentification des personnes au moyen de dispositifs biométriques dans les environnements de télécommunications) et le respect de la vie privée. Il est aussi question de l'importance de la protection de la base de données de l'annuaire.

Un chapitre présente des approches et des exemples précis relatifs à la sécurité des réseaux. Il est question, notamment, des exigences de sécurité pour les réseaux de prochaine génération, ainsi que pour les réseaux de communication mobile, lesquels sont en train de passer de l'utilisation d'une seule norme (comme le CDMA ou le GSM) à celle de plates-formes hétérogènes fonctionnant au moyen du protocole Internet. Dans le même chapitre, il est fait l'étude des dispositions de sécurité pour les réseaux domestiques, la télévision par câble et les réseaux de capteurs ubiquitaires.

Un nouveau chapitre, consacré à la cybersécurité et aux interventions en cas d'incident, a été ajouté dans la présente édition du Manuel. Pour intervenir efficacement en cas de cyberattaque, il est nécessaire de déterminer la source et la nature de l'attaque et de partager ces informations avec les organismes de surveillance. Ce chapitre traite de la mise en place d'un cadre de partage des informations relatives à la cybersécurité et des exigences concernant la détection des cyberattaques, la protection contre ces attaques, l'atténuation de leurs effets et le retour à la normale en cas de cyberattaque.

Le chapitre suivant porte sur les besoins en matière de sécurité d'un certain nombre de domaines d'application, avec un accent particulier sur les éléments de sécurité définis dans les Recommandations UIT-T. Sont notamment abordés la téléphonie IP (VoIP), la télévision utilisant le protocole Internet (TVIP) et les services web. Ce chapitre traite également des étiquettes d'identification (notamment des étiquettes d'identification par radiofréquence (RFID)), dont le déploiement est généralisé, mais qui font aussi l'objet de préoccupations grandissantes concernant les risques d'atteinte à la vie privée.

S'ensuit un exposé de mesures techniques visant à lutter contre certaines menaces courantes qui pèsent sur les réseaux, telles que le spam, les codes malveillants et les logiciels espions, ainsi qu'une présentation de l'importance de notifier et de diffuser rapidement les mises à jour des logiciels et de la nécessité de prendre en charge les incidents de sécurité de façon organisée et cohérente.

En conclusion, un bref chapitre est consacré aux futures orientations possibles des travaux de normalisation dans le domaine de la sécurité des TIC.

En fin d'ouvrage se trouve une présentation de sources d'information supplémentaires, ainsi qu'une série d'Annexes contenant les définitions des termes et la signification des acronymes utilisés dans le manuel, une présentation succincte des commissions d'études s'occupant de questions de sécurité, et la liste complète des Recommandations citées dans le Manuel. La version électronique comporte de nombreux liens vers certaines ressources et informations de vulgarisation essentielles de l'UIT-T sur la sécurité.

Introduction de la 5ème édition

Depuis la publication de la première édition du manuel, en 2003, l'UIT-T a entrepris des travaux dans un très un grand nombre de nouveaux domaines, ce qui s'est traduit par la publication de très nombreuses nouvelles Recommandations. De plus, les commissions d'études elles-mêmes ont fait l'objet d'une restructuration à la suite de l'Assemblée mondiale de normalisation des télécommunications (AMNT) de 2008.

Depuis la publication de la 4ème édition du manuel, l'élargissement des travaux a continué et le nombre de Recommandations relatives à la sécurité a augmenté, afin de répondre à la demande permanente de solutions normalisées pour s'adapter à l'évolution des menaces qui pèsent sur la sécurité des TIC. De nouveau, les éditeurs ont été confrontés à la difficulté de présenter un échantillon représentatif des travaux dans un espace limité. La 4ème édition du manuel a donné lieu à une révision importante de la structure et du contenu, ainsi qu'à l'adoption de principes directeurs concernant l'élaboration du texte. Les mêmes principes directeurs ont été suivis dans le cadre de la présente édition, si bien que la structure et le format adoptés pour la quatrième édition demeurent largement inchangés.

Ces principes directeurs, qui ont été établis à l'issue d'une consultation avec les membres de l'UIT-T, sont les suivants:

- faire en sorte que la publication attire un public large et essayer d'éviter d'employer une terminologie et des termes complexes qui risquent de n'être compris que par les spécialistes des domaines considérés;

- faire en sorte que le manuel complète les documents existants disponibles dans d'autres formats (par exemple les Recommandations) et éviter les redondances;

- rédiger le manuel de manière à pouvoir le publier à la fois en tant que document imprimé autonome et en tant que document électronique;

- employer dans le texte le plus possible de liens hypertextes vers des Recommandations et d'autres ressources accessibles au public, et faire en sorte que les informations détaillées qui ne sont pas absolument indispensables pour répondre aux objectifs de base soient accessibles par le biais de liens hypertextes; et

- faire en sorte, dans la mesure du possible, que le texte porte sur des travaux qui ont été terminés et publiés, et non sur des travaux en cours ou en projet.

Compte tenu de ces objectifs, le Manuel n'a pas pour objet de rendre compte de tous les travaux de l'UIT-T en matière de sécurité, qu'ils soient terminés ou engagés. A l'inverse, il met l'accent sur certains sujets et certaines avancées qui revêtent un caractère essentiel, et des informations supplémentaires sont accessibles par l'intermédiaire de liens hypertextes.

Le Manuel est publié à la fois en format papier et en format électronique. Les lecteurs de la version électronique ont directement accès aux Recommandations citées et aux autres documents en ligne par l'intermédiaire de liens hypertextes. Pour les lecteurs de la version papier, toutes les Recommandations mentionnées sont énumérées dans l'Annexe D et sont accessibles en ligne à l'adresse suivante: www.UIT.int/rec/T-REC/en.

Note – Le présent Manuel a un caractère purement illustratif. Il n'a aucun caractère normatif et ne remplace pas les Recommandations UIT-T qui y sont citées.

TABLE DES MATIÈRES

Page

Page

Page

1. Comment utiliser ce Manuel sur la sécurité

1 Comment utiliser ce Manuel sur la sécurité

Le présent Manuel a été élaboré pour présenter les travaux de l'UIT-T sur la sécurité des télécommunications aux cadres supérieurs et directeurs qui ont des responsabilités en ce qui concerne la sécurité des TIC et les normes associées ou qui s'intéressent à ce domaine. Il sera également utile à ceux qui souhaitent mieux comprendre les questions relatives à la sécurité des TIC et les Recommandations UIT-T qui s'y rattachent.

Le manuel donne un aperçu de la sécurité dans les télécommunications et les technologies de l'information, examine certains problèmes pratiques associés et indique comment les différents aspects de la sécurité des TIC sont abordés dans les travaux de normalisation de l'UIT-T. Il fournit des explications à caractère didactique, ainsi que des liens vers des informations plus détaillées et des documents de référence supplémentaires. En particulier, il contient des liens directs vers des Recommandations UIT-T et vers des documents de référence ou de vulgarisation associés. Il rassemble en une même publication certaines informations relatives à la sécurité figurant dans les Recommandations UIT-T et explique les relations entre les divers aspects des travaux. Il tient compte des résultats obtenus par l'UIT-T en matière de normalisation dans le domaine de la sécurité depuis la quatrième édition. Le manuel porte essentiellement sur des travaux déjà achevés. Les résultats des travaux en cours seront pris en compte dans les futures éditions du manuel.

En plus de l'UIT-T, le Secrétariat général et les autres Secteurs de l'UIT mènent aussi des travaux dans le domaine de la sécurité. On peut citer par exemple: *Understanding cybercrime: Phenomena, challenges and legal response*; *ITU national cybersecurity strategy guide*; les travaux de l'UIT-R relatifs à la sécurité des communications mobiles internationales et des services par satellite; et les travaux menés dans le cadre de l'UIT-D afin d'identifier de bonnes pratiques sur une approche nationale de la cybersécurité.

Le présent Manuel vise à donner un aperçu large et de haut niveau des activités de normalisation de l'UIT-T dans le domaine de la sécurité. Pour ceux qui souhaitent obtenir des informations plus détaillées sur les Recommandations publiées et autres documents traitant de ce domaine, des liens directs figurent dans la version électronique du texte. Le Manuel peut être utilisé de plusieurs façons. Le Tableau 1 indique comment les différentes catégories de lecteurs peuvent l'utiliser pour répondre à leurs besoins.

Tableau 1 – Comment le manuel répond aux besoins des différentes catégories de lecteurs

Organisation	Catégorie de lecteurs	Besoins	Manière dont le Manuel permet de répondre aux besoins
Fournisseurs de services de télécommunication	Cadres supérieurs/ dirigeants	Large aperçu de la portée des efforts de normalisation en matière de sécurité des TIC Feuille de route de haut niveau concernant les normes applicables en matière de sécurité des TIC	Le Manuel répond directement à ces besoins
	Ingénieurs conception et déploiement	Feuille de route concernant les normes applicables en matière de sécurité des TIC et détails techniques dans des domaines particuliers	Le Manuel fournit une feuille de route et des liens vers des explications détaillées Les Recommandations donnent des détails techniques
Vendeurs de services de télécommunication	Cadres supérieurs/ dirigeants	Large aperçu de la portée des efforts de normalisation en matière de sécurité des TIC Feuille de route de haut niveau concernant les normes applicables en matière de sécurité des TIC	Le Manuel répond directement à ces besoins
	Gestionnaires de produits	Feuille de route concernant les normes applicables	Le Manuel fournit une feuille de route et des liens vers des explications détaillées
	Conception de produit	Détails techniques dans des domaines particuliers	Le Manuel fournit des liens vers des explications détaillées dans des domaines particuliers Les Recommandations donnent des détails techniques
Utilisateurs finals	Techniques	Peuvent être intéressés par des détails techniques dans des domaines particuliers	Le Manuel fournit des liens vers des explications détaillées dans des domaines particuliers
	Non techniques	Peuvent être intéressés par un large aperçu de la portée des efforts de normalisation en matière de sécurité des TIC	Le Manuel répond directement à ces besoins
Etablissements universitaires	Etudiants/ professeurs	Feuille de route concernant les normes applicables Détails techniques dans des domaines particuliers Etre au courant des activités de normalisation nouvelles et à venir en matière de sécurité des TIC	Le Manuel fournit une feuille de route et des liens vers des explications détaillées dans des domaines particuliers
Pouvoirs publics	Cadres supérieurs et dirigeants Régulateurs Décideurs	Large aperçu de la portée des efforts de normalisation en matière de sécurité des TIC Feuille de route de haut niveau concernant les normes applicables en matière de sécurité des TIC	Le Manuel répond directement à ces besoins
Organisations non gouvernementales	Cadres supérieurs /dirigeants	Large aperçu de la portée des efforts de normalisation en matière de sécurité des TIC Feuille de route de haut niveau concernant les normes applicables en matière de sécurité des TIC	Le Manuel répond directement à ces besoins
	Perfectionnement et renforcement des capacités	Feuille de route concernant les normes applicables en matière de sécurité des TIC Détails techniques dans des domaines particuliers	Le Manuel fournit des liens vers des explications détaillées dans des domaines particuliers Les Recommandations donnent des détails techniques

2. Aperçu des activités de l'UIT-T dans le domaine de la sécurité

2 Aperçu des activités de l'UIT-T dans le domaine de la sécurité

L'UIT-T travaille dans le domaine de la sécurité des TIC depuis plus de trente ans, période pendant laquelle plusieurs commissions d'études ont élaboré des Recommandations et des orientations dans un certain nombre de domaines essentiels. Les travaux de l'UIT-T sur la sécurité des TIC sont maintenant essentiellement du ressort de la Commission d'études 17 (CE 17), qui a été désignée Commission d'études directrice pour la sécurité. Toutefois, il existe des aspects liés à la sécurité dans la plupart des domaines étudiés par l'UIT-T, et la plupart des commissions d'études mènent des travaux sur la sécurité en lien avec leur propre domaine de compétence.

En sa qualité de Commission d'études directrice pour la sécurité, la CE 17 a élaboré un certain nombre de publications de référence et de vulgarisation. Ces publications, qui comprennent le présent Manuel, facilitent la coordination des travaux sur la sécurité au sein de l'UIT-T, et contribuent à promouvoir ces travaux auprès d'une communauté beaucoup plus large et à encourager l'utilisation des Recommandations.

Le présent chapitre expose de manière succincte les principaux thèmes liés à la sécurité et cite des exemples de Recommandations relatives à ce domaine. Il oriente également le lecteur vers des sources d'information supplémentaires concernant les publications de vulgarisation et les travaux actuellement en cours.

2.1 Documents de référence et de vulgarisation

L'UIT-T tient à jour un certain nombre de publications et de sites web à partir desquels il est possible d'obtenir des informations plus détaillées sur les Recommandations et les travaux de l'UIT-T dans le domaine de la sécurité.

On trouvera sur le site web de la Commission d'études 17 un résumé des attributions et des activités de cette Commission d'études, ainsi qu'une brève description des documents, y compris les documents de vulgarisation, avec des liens vers lesdits documents, des informations sur les ateliers passés, les exposés et les activités de vulgarisation, et des liens vers des orientations en matière de sécurité des TIC, y compris un exposé didactique sur l'écriture de programmes sûrs et sécurisés.

Pour plus de plus amples informations sur divers aspects des travaux relatifs à la sécurité, on se reportera au Chapitre 13, qui contient également des liens directs vers d'autres informations.

2.2 Aperçu de sujets essentiels liés à la sécurité et des Recommandations associées

Le Tableau 2 constitue un aide-mémoire de certains des principaux sujets liés à la sécurité et des Recommandations associées examinés dans le présent Manuel. Les lecteurs qui utilisent la version électronique du Manuel y trouveront des liens hypertextes vers le texte relatif à chaque sujet et sous-sujet, ainsi que vers les Recommandations énumérées. L'Annexe D contient la liste complète des Recommandations citées dans le présent Manuel, et dans la version électronique se trouvent des liens hypertextes qui permettent d'accéder directement à ces Recommandations et de les télécharger.

Tableau 2 – Aperçu de certains sujets essentiels et de certaines Recommandations (Partie 1/3)

Sujet	Sous-sujet	Exemples de Recommandations et publications associées	
Exigences de sécurité	Menaces, risques et vulnérabilité (3.2) Exigences de sécurité du personnel et de sécurité physique (3.6) Réseaux de prochaine génération (8.1) Exigences de sécurité pour IPCablecom (8.4) TVIP (10.2)	UIT-T E.408 UIT-T X.1051 UIT-T Y.2701 UIT-T Y.2740 UIT-T J.170 UIT-T X.1191	*Prescriptions de sécurité des réseaux de télécommunication* *Technologies de l'information – Techniques de sécurité - Lignes directrices basées sur la norme ISO/CEI 27002 pour la gestion de la sécurité des informations pour les organisations de télécommunication* *Prescriptions de sécurité des réseaux de prochaine génération de version 1* *Spécifications de sécurité applicables aux transactions financières mobiles à distance dans les réseaux de prochaine génération* *Spécification de la sécurité sur IPCablecom* *Spécifications fonctionnelles et architecture concernant les aspects de sécurité de la TVIP*
Architectures de sécurité	Architecture de sécurité pour les systèmes ouverts (4.1) Services de sécurité (4.2) Architecture de sécurité pour les communications de bout en bout (4.3) Disponibilité du réseau et de ses composants (4.3.2) Architectures propres à certaines applications (4.5) Architectures de sécurité d'homologue à homologue (4.6) Sécurité des messages (4.5.2) Architecture de gestion de réseau (7.2) Architecture IPCablecom (8.4.1) TVIP (10.2)	UIT-T X.800 UIT-T X.810 UIT-T X.805 UIT-T G.827 UIT-T X.1162 UIT-T X.1161 UIT-T X.1143 UIT-T M.3010 UIT-T J.160 UIT-T X.1191	*Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT* *Cadres de sécurité pour les systèmes ouverts: aperçu général* *Architecture de sécurité pour les systèmes assurant des communications de bout en bout* *Paramètres et objectifs de disponibilité pour les conduits numériques internationaux de bout en bout à débit constant* *Architecture de sécurité et opérations dans les réseaux entre homologues* *Cadre applicable aux communications sécurisées entre homologues* *Architecture de sécurité des messages dans l'environnement des services web mobiles* *Principes des réseaux de gestion des télécommunications* *Cadre architectural pour l'acheminement de services à temps critique sur des réseaux de télévision par câble utilisant des câblo-modems* *Spécifications fonctionnelles et architecture concernant les aspects de sécurité de la TVIP*
Gestion de la sécurité	Gestion de la sécurité des informations (5.1) Gestion des risques (5.2) Traitement des incidents (5.3) Gestion des actifs (5.4)	UIT-T X.1051 UIT-T X.1052 UIT-T X.1055 UIT-T E.409 UIT-T X.1057	*Technologies de l'information – Techniques de sécurité – Lignes directrices basées sur la norme ISO/CEI 27002 pour la gestion de la sécurité des informations pour les organisations de télécommunication* *Cadre de gestion de la sécurité de l'information* *Lignes directrices relatives à la gestion des risques et aux profils de risques pour les organisations de télécommunication* *Organisation en cas d'incident et prise en charge des incidents relatifs à la sécurité: lignes directrices destinées aux organisations de télécommunication* *Lignes directrices relatives à la gestion des actifs dans les organisations de télécommunication*

Tableau 2 – Aperçu de certains sujets essentiels et de certaines Recommandations (Partie 2/3)

Sujet	Sous-sujets	Exemples de Recommandations et publications associées	
L'annuaire, authentification et gestion d'identité	Concepts liés à l'annuaire (6) Protection des informations de l'annuaire (6.1) Mécanismes de sécurité à clé publique (6.2) Protection de la confidentialité (6.1.4) Gestion d'identité (6.4) Terminologie relative à la gestion d'identité (6.4.2) Authentification télébiométrique (6.5.1) Aspects de sécurité et d'innocuité de la télébiométrie (6.5.3)	UIT-T X.500	*L'annuaire: aperçu général des concepts, modèles et services*
		UIT-T X.509	*L'annuaire: cadre général des certificats de clé publique et d'attribut*
		UIT-T X.1171	*Menaces et protection requise pour les informations d'identification personnelle dans les applications utilisant l'identification par étiquette*
		UIT-T X.1250	*Capacités de base pour l'amélioration de l'interopérabilité globale dans la gestion d'identité*
		UIT-T X.1251	*Cadre de contrôle de l'identité numérique par l'utilisateur*
		UIT-T X.1253	*Lignes directrices pour la sécurité des systèmes de gestion d'identité*
		UIT-T Y.2720	*Cadre de gestion d'identité dans les NGN*
		UIT-T Y.2722	*Mécanismes de gestion d'identité dans les réseaux de prochaine génération*
		UIT-T X.1252	*Termes et définitions de base relatifs à la gestion d'identité*
		UIT-T X.1084	*Mécanisme de système télébiométrique – Partie 1: Protocole général d'authentification biométrique et profils types pour les systèmes de télécommunication*
		UIT-T X.1089	*Infrastructure d'authentification télébiométrique*
		UIT-T X.1081	*Le modèle télébiométrique multimodal – Cadre général pour la spécification des aspects de sécurité et d'innocuité de la télébiométrie*
Sécurisation de l'infrastructure de réseau	Le réseau de gestion des télécommunications (7.1) Sécurisation des activités de surveillance et de contrôle (7.4) Sécurisation des activités d'exploitation de réseau et des applications de gestion de réseau (7.5) Services communs de gestion de la sécurité (7.6) Services de sécurité fondés sur l'architecture CORBA (7.6.4)	UIT-T M.3010	*Principes du réseau de gestion des télécommunications*
		UIT-T M.3016.0	*Sécurité pour le plan de gestion: aperçu général*
		UIT-T M.3210.1	*Services de gestion RGT pour la gestion de la sécurité des réseaux IMT-2000*
		UIT-T X.790	*Fonction de gestion des dérangements pour les applications de l'UIT-T*
		UIT-T X.711	*Protocole commun d'information de gestion: spécification*
		UIT-T X.736	*Gestion-systèmes: fonction de signalisation des alarmes de sécurité*
		UIT-T X.740	*Gestion-systèmes: fonction de piste de vérification de sécurité*
		UIT-T X.780	*Directives concernant le RGT pour la définition d'objets gérés CORBA*
Approches particulières relatives à la sécurité des réseaux	Sécurité des réseaux de prochaine génération (NGN) (8.1) Sécurité des communications mobiles (8.2) Sécurité des réseaux domestiques (8.3) Sécurité des réseaux de capteurs ubiquitaires (8.6)	UIT-T Y.2001	*Aperçu général des réseaux de prochaine génération*
		UIT-T Y.2701	*Prescriptions de sécurité des réseaux de prochaine génération de version 1*
		UIT-T X.1121	*Cadre général des technologies de la sécurité pour les communications mobiles de données de bout en bout*
		UIT-T X.1111	*Cadre général des technologies de sécurité pour les réseaux domestiques*
		UIT-T X.1311	*Cadre de sécurité des réseaux de capteurs ubiquitaires*

Tableau 2 – Aperçu de certains sujets essentiels et de certaines Recommandations (Partie 3/3)

Sujet	Sous-sujets	Exemples de Recommandations et publications associées	
Cybersécurité et intervention en cas d'incident	Echange d'informations sur la cybersécurité (9.1)	UIT-T X.1205	*Aperçu général de la cybersécurité*
		UIT-T X.1500	*Aperçu général de l'échange d'informations sur la cybersécurité*
	Echange d'informations de vulnérabilité (9.1.3)	UIT-T X.1520	*Vulnérabilités et expositions courantes*
		UIT-T X.1570	*Mécanismes de découverte dans le cadre de l'échange d'informations de cybersécurité*
	Découverte d'informations de cybersécurité (9.1.5)	UIT-T E.409	*Organisation en cas d'incident et prise en charge des incidents relatifs à la sécurité: lignes directrices destinées aux organisations de télécommunication*
	Traitement des incidents (9.2)	UIT-T X.1056	*Lignes directrices relatives à la gestion des incidents de sécurité dans les organisations de télécommunication*
Sécurité des applications	Téléphonie IP (VoIP) et multimédia (10.1)	UIT-T H.235	*Cadre de sécurité H.323: cadre de sécurité pour les systèmes multimédias de la série H (systèmes H.323 et autres systèmes de type H.245)*
	TVIP (10.2)	UIT-T X.1195	*Mécanisme d'interopérabilité de la protection de service et de contenu*
		UIT-T T.36	*Capacités de sécurité à utiliser avec les télécopieurs du Groupe 3*
	Transmission de télécopie sécurisée (10.3)	UIT-T X.1141	*Langage de balisage d'assertion de sécurité (SAML 2.0)*
		UIT-T X.1142	*Langage de balisage extensible pour le contrôle d'accès (XACML 2.0)*
	Services web (10.4)	UIT-T X.1171	*Menaces et protection requise pour les informations d'identification personnelle dans les applications utilisant l'identification par étiquette*
	Services par étiquette (10.5)		
Lutte contre les menaces courantes dans les réseaux	Spam (11.1)	UIT-T X.1231	*Stratégies techniques de lutte contre le spam*
		UIT-T X.1241	*Cadre technique pour lutter contre les spams par courrier électronique*
		UIT-T X.1244	*Aspects généraux de la lutte contre le spam dans les applications multimédias sur les réseaux IP*
	Codes malveillants, logiciels espions et logiciels trompeurs (11.2)	UIT-T X.1207	*Lignes directrices à l'intention des fournisseurs de services de télécommunication pour lutter contre les risques d'installation de logiciels espions ou de tout logiciel potentiellement indésirable*
	Notification et diffusion de mises à jour de logiciels (11.3)	UIT-T X.1206	*Cadre de notification automatique d'informations liées à la sécurité et de diffusion de mises à jour, indépendant du fournisseur*
Le Tableau ci-dessus illustre *certains* des sujets et Recommandations dont il est question dans le présent Manuel. Il ne vise pas à l'exhaustivité. On trouvera dans l'Annexe D la liste complète des Recommandations relatives à la sécurité citées dans l'ouvrage. L'ensemble complet des Recommandations UIT-T est accessible à l'adresse suivante: http://www.UIT.int/UIT-T/recommendations/. Les numéros figurant entre parenthèses après chaque sous-sujet correspondent aux paragraphes du Manuel dans lesquels ces sous-sujets sont traités.			

3. Exigences de sécurité

3 Exigences de sécurité

Pour élaborer un cadre de sécurité, quel qu'il soit, il est très important d'avoir une idée claire des exigences. Un tour d'horizon complet des exigences de sécurité doit prendre en compte: les parties concernées, les actifs nécessitant une protection, les menaces vis-à-vis desquelles ces actifs doivent être protégés, les vulnérabilités associées aux actifs et à l'environnement et le risque global encouru par les actifs compte tenu de ces menaces et vulnérabilités.

Le présent Chapitre donne un aperçu des exigences de base pour la protection des applications des TIC, des services et des informations, explicite les menaces et les vulnérabilités sur lesquelles reposent les exigences, examine le rôle des normes dans le respect des exigences et identifie certains aspects nécessaires pour protéger les diverses parties impliquées dans l'utilisation et dans l'exploitation de fonctionnalités des TIC.

Les exigences de sécurité sont génériques ou dépendantes du contexte. Qui plus est, certaines exigences sont bien établies alors que d'autres continuent à évoluer à mesure que de nouvelles applications apparaissent et que l'environnement des menaces évolue. Le présent chapitre porte essentiellement sur les exigences génériques, les exigences applicables à des applications ou des environnements particuliers étant examinées dans d'autres chapitres.

3.1 Menaces, risques et vulnérabilités

D'une manière générale, dans le domaine de la sécurité des TIC, les parties pouvant nécessiter une protection des actifs sont les suivantes:

- *les clients/abonnés*, qui veulent que le réseau et les services offerts soient fiables et que les services soient disponibles (notamment les services d'urgence);
- *la communauté/les autorités publiques*, qui exigent que la sécurité fasse l'objet de directives et/ou de lois, afin de garantir la disponibilité des services, une concurrence loyale et la protection de la vie privée; et
- *les opérateurs de réseau et les fournisseurs de services*, qui ont besoin de sécurité pour sauvegarder leurs intérêts opérationnels et commerciaux et pour satisfaire à leurs obligations vis-à-vis de leurs clients, de leurs partenaires commerciaux et du public.

Les actifs à protéger sont les suivants:

- services de communication et services informatiques;
- informations et données, notamment les logiciels et les données concernant les services de sécurité;
- personnel; et
- équipements et installations.

Une *menace de sécurité* est définie comme étant une violation potentielle de la sécurité, par exemple:

- divulgation non autorisée d'informations;
- destruction ou modification non autorisée de données, d'équipements ou d'autres ressources;
- vol, suppression ou perte d'informations ou d'autres ressources;

- interruption ou déni de services; et
- usurpation de l'identité d'une entité autorisée.

Les menaces peuvent être *accidentelles* (auquel cas on parle aussi parfois de menaces *non intentionnelles*) ou *délibérées* et peuvent être *actives* ou *passives*. Une menace accidentelle est une menace sans préméditation (par exemple dysfonctionnement d'un système ou d'un logiciel ou défaillance physique). Une menace délibérée est une menace dont la mise à exécution est un acte délibéré commis par une personne. Les menaces délibérées vont de l'examen occasionnel à l'aide d'outils de surveillance faciles d'accès, à des attaques sophistiquées reposant sur une connaissance spéciale du système. Lorsqu'une menace délibérée est mise à exécution, on parle alors d'*attaque*. Une menace active est une menace résultant d'une modification de l'état ou du fonctionnement d'un système (par exemple altération de données ou destruction d'un équipement physique). Pour une menace passive, il n'y a pas de modification d'état (par exemple écoute clandestine).

Une *vulnérabilité de sécurité* est un défaut ou une faille susceptible d'être exploité pour violer un système ou les informations qu'il contient. Si une vulnérabilité existe, il est alors possible qu'une menace soit mise à exécution, à moins qu'il ne soit prévu des contre-mesures efficaces.

Dans les Recommandations UIT-T, quatre types de vulnérabilité sont pris en considération:

- les vulnérabilités du modèle des menaces, qui résultent de l'incapacité de prévoir les éventuelles menaces futures;
- les vulnérabilités de conception et de spécification, qui proviennent d'erreurs ou d'oublis dans la conception d'un système ou d'un protocole qui le rendent intrinsèquement vulnérable;
- les vulnérabilités de mise en œuvre, qui résultent d'erreurs ou d'oublis au cours de la mise en œuvre d'un système ou d'un protocole; et
- les vulnérabilités d'exploitation et de configuration, qui proviennent d'un mauvais usage d'options dans des mises en œuvre ou de politiques et de pratiques de déploiement déficientes (par exemple la non-utilisation du chiffrement dans un réseau sans fil).

Le *risque de sécurité* est une mesure des effets négatifs qui peuvent se produire en cas d'exploitation d'une vulnérabilité de sécurité, autrement dit si une menace est mise à exécution. Le risque ne peut jamais être éliminé, mais un objectif de la sécurité est de réduire le risque à un niveau acceptable. Pour cela, il faut comprendre les menaces et les vulnérabilités applicables et appliquer des contre-mesures appropriées. Il s'agit généralement de services et de mécanismes de sécurité auxquels peuvent s'ajouter des mesures non techniques (sécurité physique et sécurité du personnel par exemple).

Alors que les menaces et les agents responsables de menaces changent, les vulnérabilités de sécurité existent pendant toute la durée de vie d'un système ou d'un protocole, sauf si des mesures spécifiques sont prises pour y faire face. Les protocoles normalisés étant très largement utilisés, toute vulnérabilité associée à un protocole peut avoir des conséquences très graves et concerner le monde entier. Il est donc particulièrement important de comprendre et de détecter les vulnérabilités présentes dans les protocoles et de prendre des mesures pour y faire face une fois qu'elles ont été détectées.

Les organismes de normalisation ont à la fois une certaine responsabilité et une compétence unique pour ce qui est de faire face aux vulnérabilités de sécurité susceptibles d'être présentes dans des spécifications d'architectures, de cadres, de protocoles, etc. Même avec une bonne connaissance des menaces, des risques et des vulnérabilités associés aux réseaux informatiques et aux réseaux de télécommunication, il est impossible d'obtenir une sécurité correcte si on n'applique pas systématiquement des mesures de sécurité conformément aux politiques de sécurité en vigueur, lesquelles doivent être examinées et mises à jour régulièrement. Il faut aussi prévoir correctement la gestion de la sécurité et l'intervention en d'incidents, par exemple déterminer

les responsabilités et les mesures à prendre concernant la prévention, la détection, l'examen et la prise en charge des incidents de sécurité.

Des services et des mécanismes de sécurité peuvent protéger les réseaux de télécommunication contre les attaques malveillantes telles que le déni de service, l'écoute clandestine, l'usurpation d'identité, l'altération des messages (modification, retard, suppression, insertion, relecture, réacheminement, déroutement ou réordonnancement de messages), la répudiation ou la falsification. Les techniques de protection comprennent la prévention et la détection des attaques et le retour à la normale après une attaque ainsi que la gestion des informations liées à la sécurité. La protection doit comprendre des mesures visant à empêcher les interruptions de service dues à des événements naturels (tempêtes et séismes par exemple) ou à des attaques malveillantes (actes délibérés ou violents). Des dispositions doivent aussi être prises pour faciliter l'interception et la surveillance par les autorités judiciaires dûment autorisées.

La sécurité des réseaux de télécommunication nécessite également une large coopération entre les fournisseurs de services. La Recommandation UIT-T E.408 donne un aperçu général des exigences de sécurité et définit un cadre qui identifie les menaces de sécurité dans les réseaux de télécommunication en général (fixes et mobiles; voix et données) et qui indique comment planifier des contre-mesures afin de limiter les risques découlant de ces menaces. La mise en application des exigences énoncées dans la Recommandation UIT-T E.408 favorisera la coopération internationale dans les domaines ci-après concernant la sécurité des réseaux de télécommunication:

- partage et diffusion des informations;
- coordination en cas d'incident et réaction en cas de crise;
- recrutement et formation de professionnels de la sécurité;
- coordination de l'application de la loi;
- protection des infrastructures et services critiques; et
- élaboration d'une législation appropriée.

Toutefois, pour faciliter cette coopération, il est essentiel d'appliquer les exigences concernant les composants nationaux du réseau.

La Recommandation UIT-T X.1205 décrit les différentes menaces de sécurité du point de vue d'une organisation et examine les menaces dans les diverses couches d'un réseau.

3.2 Objectifs généraux de sécurité pour les réseaux TIC

Les objectifs généraux de sécurité pour les réseaux TIC sont les suivants:

a) l'accès aux services et aux réseaux, ainsi que leur utilisation, devraient être limités aux utilisateurs autorisés;

b) les utilisateurs autorisés devraient pouvoir accéder aux actifs pour lesquels ils disposent d'une autorisation d'accès et opérer sur ces actifs;

c) les réseaux devraient offrir un niveau de confidentialité conforme aux exigences des politiques de sécurité qui leurs sont applicables;

d) toutes les entités de réseau devraient être tenues responsables de leurs actions et uniquement de leurs actions;

e) les réseaux devraient être protégés contre les accès et les opérations non sollicités;

f) des informations relatives à la sécurité devraient être accessibles sur le réseau, mais uniquement pour les utilisateurs autorisés;

g) des plans devraient être établis afin de fixer les modalités de prise en charge des incidents de sécurité;

h) des procédures devraient être prévues afin d'assurer le retour à la normale à la suite de la détection d'une atteinte à la sécurité; et

i) l'architecture de réseau devrait permettre l'application de différentes politiques de sécurité et l'utilisation de mécanismes de sécurité plus ou moins stricts.

Afin d'atteindre ces objectifs, il convient d'apporter une grande attention à la sécurité lors de la conception, de la mise en œuvre et de l'exploitation des réseaux. Il importe également d'élaborer des politiques de sécurité, de fournir des services de sécurité appropriés et de gérer les risques de manière cohérente et permanente.

3.3 Raison d'être des normes sur la sécurité

L'utilisation de normes adoptées à l'échelle internationale pour servir de base à la sécurité des réseaux permet d'encourager des approches communes et de faciliter l'interconnexion, et s'avère plus rentable que l'élaboration d'approches individuelles pour chaque juridiction.

Dans certains cas, la mise en place et l'utilisation de services et de mécanismes de sécurité peuvent s'avérer relativement onéreuses par rapport à la valeur des actifs protégés. Il est donc important de pouvoir adapter les services et les mécanismes de sécurité aux besoins locaux. Toutefois, la possibilité d'adapter la sécurité peut aussi donner lieu à un certain nombre de combinaisons possibles de fonctions de sécurité. Par conséquent, il est souhaitable de disposer de *profils de sécurité* qui couvrent une grande variété de réseaux et services de télécommunication afin d'harmoniser les options dans les différentes mises en œuvre. La normalisation et l'utilisation de profils normalisés facilitent l'interopérabilité et 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 de sécurité de réseau normalisées présentent des avantages à la fois pour les fournisseurs de produits et pour les fournisseurs de services, car elles permettent de réaliser des économies d'échelle lors de l'élaboration des produits et d'assurer l'interopérabilité des composants.

3.4 Evolution des normes de l'UIT-T sur la sécurité

Les travaux menés par l'UIT-T dans le domaine de la sécurité continuent d'évoluer, afin de répondre aux exigences des membres de l'UIT-T. On aborde ici certains aspects essentiels de cette évolution, plus particulièrement en ce qui concerne les exigences de sécurité. On trouvera plus de détails sur certaines Recommandations plus loin dans le Manuel.

D'une manière générale, les exigences de sécurité des TIC sont définies sur la base des menaces qui pèsent sur le réseau et/ou le système, des vulnérabilités intrinsèques au réseau et/ou au système et des mesures qu'il faut prendre pour lutter contre les menaces et réduire les vulnérabilités. Les exigences de protection concernent le réseau et ses composants. Les concepts fondamentaux liés à la sécurité, y compris les menaces, les vulnérabilités et les contre-mesures de sécurité, sont définis dans la Recommandation UIT-T X.800, publiée en 1991. La Recommandation UIT-T E.408, que nous avons déjà mentionnée et qui a été publiée en 2004, s'appuie sur les concepts et la terminologie de la Recommandation UIT-T X.800. Elle présente un caractère général et n'expose pas d'exigences relatives à des réseaux particuliers ni ne traite de nouveaux services de sécurité. A l'inverse, cette Recommandation met l'accent sur l'utilisation de services de sécurité existants définis dans d'autres Recommandations UIT-T et dans des normes élaborées par d'autres organismes.

La nécessité de lutter contre des menaces de cybersécurité toujours plus nombreuses et plus diverses (virus, vers, chevaux de Troie, attaques par usurpation d'identité, vol d'identité, spam et autres formes de cyberattaque) est prise en compte dans la Recommandation UIT-T X.1205, publiée en 2008. Cette Recommandation a pour objet d'élaborer une base de connaissances qui puisse faciliter la sécurisation des réseaux de demain. Elle traite de diverses contre-mesures visant à remédier aux menaces: routeurs, pare-feu, protection antivirus, systèmes de détection des intrusions, systèmes de protection contre les intrusions, informatique sécurisée, audit et surveillance, etc. Elle aborde les principes de protection des réseaux, par exemple la défense en profondeur et la gestion d'accès. Elle traite des stratégies et techniques de gestion des risques, y compris de l'importance de la formation et de la sensibilisation à la protection du réseau. En outre, des exemples sont fournis concernant la sécurisation de divers réseaux compte tenu des techniques présentées.

La Recommandation UIT-T X.1205 définit la cybersécurité comme étant "l'ensemble des outils, politiques, concepts de sécurité, mécanismes de sécurité, lignes directrices, méthodes de gestion des risques, actions, formations, bonnes pratiques, garanties et technologies qui peuvent être utilisés pour protéger le cyberenvironnement et les actifs des organisations et des utilisateurs". Ces actifs comprennent les dispositifs informatiques connectés, les utilisateurs de l'informatique, les applications/services, les systèmes de communication, les communications multimédias et la totalité des informations transmises et/ou stockées dans le cyberenvironnement. Telle qu'elle est définie dans cette Recommandation, la cybersécurité a pour objet de garantir que les propriétés de sécurité des organisations (disponibilité, intégrité et confidentialité) sont assurées et maintenues et de protéger les actifs des utilisateurs contre les risques qui pèsent sur la sécurité dans le cyberenvironnement.

Dans l'environnement actuel des entreprises, le concept de périmètre disparaît. Les frontières entre réseau interne et réseau externe sont de plus en plus minces. Les applications fonctionnent sur les réseaux sur la base de couches. La sécurité doit absolument être garantie à l'intérieur de chacune de ces couches et entre elles. Une approche de la sécurité par couches permet aux organisations de créer plusieurs niveaux de défense contre les menaces.

Des techniques de cybersécurité peuvent être utilisées pour garantir la disponibilité des systèmes, l'intégrité, l'authenticité, la confidentialité et la non-répudiation, pour garantir le respect de la vie privée des utilisateurs ainsi que pour établir la fiabilité des utilisateurs. Parmi les techniques de cybersécurité les plus importantes actuellement utilisées, on peut citer:

– la cryptographie, qui permet d'assurer un certain nombre de services de sécurité, notamment la confidentialité des données au cours de leur transmission ou durant leur stockage, ainsi qu'une signature électronique;

– les contrôles d'accès, qui visent à protéger les informations contre un accès ou une utilisation non autorisée;

– l'intégrité des systèmes et des données, dont le but est de garantir qu'un système et ses données ne sont pas modifiés ou altérés par des parties non autorisées, ou de manière non autorisée;

– l'audit, la journalisation et la surveillance, qui fournissent des informations permettant d'évaluer l'efficacité de la stratégie et des techniques de sécurité employées;

– la gestion de la sécurité, qui inclut la configuration de la sécurité, les contrôles de sécurité, la gestion des risques, le traitement des incidents et la gestion des informations relatives à la sécurité.

Les organisations doivent mettre au point un plan de sécurité détaillé adapté à chaque contexte particulier. La sécurité n'est pas "à taille unique". Elle doit être prise en considération dans le cadre d'un processus permanent assurant la protection des systèmes, des données, des réseaux, des applications et des ressources. Elle doit en outre englober toutes les couches d'un système. L'adoption d'une approche de la sécurité par couches conjuguée à une gestion et à une application de politiques efficaces permet d'offrir un ensemble de solutions de sécurité qui peuvent être modulaires, souples et évolutives.

3.5 Exigences de sécurité du personnel et de sécurité physique

Les Recommandations UIT-T relatives à la sécurité portent essentiellement sur les aspects techniques des systèmes et des réseaux. Certains aspects de sécurité du personnel sont traités dans la Recommandation UIT-T X.1051. La sécurité physique est également une dimension très importante de la protection mais elle entre peu dans le cadre des travaux de l'UIT-T. Toutefois, des exigences générales de sécurité physique sont énoncées dans la Recommandation UIT-T X.1051 et la sécurité physique des installations extérieures est abordée dans les deux documents mentionnés ci-dessous.

En ce qui concerne la protection physique des installations extérieures, il s'agit notamment de faire en sorte que les matériels puissent résister aux menaces d'incendie, de catastrophe naturelle et de dommages intentionnels ou accidentels. Des méthodes de protection des composants, câbles, enceintes, armoires, etc., sont décrites dans le *Manuel de l'UIT-T sur les technologies des installations extérieures appliquées aux réseaux publics* et le *Manuel de l'UIT-T sur l'application des ordinateurs et des microprocesseurs à la fabrication,à l'installation et à la protection des câbles de télécommunication*. Ces documents traitent également de la surveillance des systèmes afin de prévenir les dommages et indiquent la marche à suivre pour remédier aux problèmes et rétablir la fonctionnalité des systèmes le plus rapidement possible.

4. Architectures de sécurité

4 Architectures de sécurité

Les architectures de sécurité, et les modèles et cadres associés, constituent une structure et un contexte dans le cadre desquels des normes techniques connexes peuvent être élaborées de manière cohérente. Au début des années 80, il s'est avéré nécessaire de disposer d'un cadre dans lequel la sécurité pourrait être appliquée dans une architecture de communications en couches, ce qui a motivé l'élaboration de la Recommandation UIT-T X.800, première d'une série de normes définissant des architectures pour les services et les mécanismes de sécurité. Ces travaux, menés en grande partie en collaboration avec l'ISO, ont conduit à d'autres normes, notamment sur des modèles et des cadres de sécurité qui spécifient comment des types de protection particuliers peuvent être appliqués dans des environnements particuliers.

Plus tard, il s'est avéré nécessaire de définir des architectures de sécurité génériques et des architectures de sécurité propres à certaines applications, ce qui a conduit à l'élaboration de la Recommandation UIT-T X.805, ainsi qu'à un certain nombre d'architectures propres à certaines applications, par exemple la gestion de réseau, les communications entre homologues et les serveurs web mobiles. La Recommandation UIT-T X.805, qui est décrite plus loin dans le présent chapitre, complète les autres Recommandations UIT-T de la série X.800, en offrant des solutions de sécurité destinées à assurer la sécurité de réseau de bout en bout.

4.1 Architecture de sécurité pour les systèmes ouverts et normes associées

La première des architectures de sécurité pour les communications à avoir été normalisée a été l'architecture de sécurité pour les systèmes ouverts, définie dans la Recommandation UIT-T X.800. Cette Recommandation définit les éléments d'architecture liés à la sécurité qui peuvent être appliqués en fonction des conditions dans lesquelles une protection est requise. Elle contient en particulier une description générale de services de sécurité et des mécanismes associés qui peuvent être utilisés pour assurer les services. Elle définit aussi, sur la base du modèle de référence de base à sept couches pour l'interconnexion des systèmes ouverts (OSI, *open systems interconnection*), les emplacements les plus appropriés (c'est-à-dire les couches) pour implémenter les services de sécurité.

La Recommandation UIT-T X.800 porte uniquement sur les aspects visibles d'une voie de communication permettant aux systèmes d'extrémité de se transférer des informations en toute sécurité. Elle ne vise pas à spécifier des mises en œuvre particulières et elle ne définit pas la marche à suivre pour évaluer la conformité d'une mise en œuvre donnée à cette norme sur la sécurité ou à toute autre norme sur la sécurité. Elle ne précise pas non plus les mesures de sécurité additionnelles qui pourraient être nécessaires dans les systèmes d'extrémité pour prendre en charge les fonctionnalités de sécurité des communications.

L'architecture de sécurité définie dans la Recommandation UIT-T X.800 a été élaborée spécifiquement pour les systèmes OSI, mais les concepts sous-jacents se sont avérés avoir une applicabilité et une acceptation beaucoup plus larges. La norme est particulièrement importante car elle représente le premier consensus à l'échelle internationale sur les définitions des services de sécurité de base (*authentification*, *contrôle d'accès*, *confidentialité des données*, *intégrité des données* et *non-répudiation*) ainsi que de services plus généraux (omniprésents) (*fonctionnalité de confiance*, *détection d'événements*, *audit de sécurité et reprise de sécurité*, etc.). Elle indique également les mécanismes de sécurité qui peuvent être utilisés pour fournir les services de sécurité. Avant l'élaboration de la Recommandation UIT-T X.800, les avis étaient très partagés sur les services de sécurité de base nécessaires et sur les fonctions exactes de chaque service. L'intérêt et l'applicabilité générale de la Recommandation UIT-T X.800 tiennent au fait que cette Recommandation représente un consensus international important sur la signification des termes employés pour décrire les fonctionnalités de sécurité, sur l'ensemble des services de sécurité nécessaires pour assurer la protection des communications de données et sur la nature de ces services de sécurité.

Au cours de l'élaboration de la Recommandation UIT-T X.800, il s'est avéré nécessaire d'établir d'autres normes connexes sur la sécurité des communications. Un certain nombre de normes connexes et de Recommandations complémentaires relatives à l'architecture ont donc commencé à être mises au point. Certaines de ces Recommandations sont examinées ci-après.

4.2 Services de sécurité

Des cadres de sécurité ont été élaborés afin de décrire de façon complète et cohérente chacun des services de sécurité définis dans la Recommandation UIT-T X.800. Ils ont pour objet de définir tous les aspects liés à l'application des services de sécurité dans le contexte d'une architecture de sécurité particulière, y compris les éventuelles architectures de sécurité qui seront définies dans le futur. Ces cadres visent essentiellement à assurer la protection des systèmes, des objets contenus dans les systèmes et de l'interaction entre les systèmes. Ils ne traitent pas de la marche à suivre pour construire des systèmes ou des mécanismes. La Recommandation ITU-T X.810 présente les différents cadres et décrit les concepts communs (domaines de sécurité, autorités de sécurité et politiques de sécurité) qui sont utilisés dans tous les cadres. Elle décrit également un format de données générique qui peut être utilisé pour acheminer en toute sécurité les informations d'authentification et de contrôle d'accès.

L'*authentification* est l'attestation de l'identité revendiquée par une entité. Les entités incluent non seulement les utilisateurs humains, mais aussi les dispositifs, les services et les applications. L'authentification permet aussi d'attester qu'une entité ne tente pas d'usurper l'identité d'une autre entité ni de reprendre sans autorisation une communication précédente. La Recommandation UIT-T X.800 définit deux formes d'authentification: *l'authentification de l'origine des données* (à savoir la confirmation que la source des données reçues est telle que déclarée) et *l'authentification de l'entité homologue* (à savoir la confirmation qu'une entité homologue d'une association est bien l'entité déclarée). La Recommandation UIT-T X.811 définit les concepts de base de l'authentification, différentes classes de mécanismes d'authentification, les services correspondant à ces classes de mécanismes, les exigences fonctionnelles que les protocoles doivent respecter pour prendre en charge ces classes de mécanismes et, enfin, les exigences générales de gestion concernant l'authentification.

Le *contrôle d'accès* est la précaution prise contre l'utilisation non autorisée d'une ressource, y compris la précaution prise contre l'utilisation d'une ressource de façon non autorisée. 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'informations, aux services et aux applications. La Recommandation UIT-T X.812 décrit un modèle incluant tous les aspects du contrôle d'accès dans les systèmes ouverts, la relation avec les autres fonctions de sécurité (par exemple l'authentification et l'audit) et les exigences de gestion concernant le contrôle d'accès.

La *non-répudiation* est la capacité d'empêcher les entités de nier ultérieurement qu'elles ont exécuté une action. Il s'agit d'établir une preuve qui puisse ensuite être utilisée pour rejeter les fausses déclarations. La Recommandation UIT-T X.800 décrit deux formes de service de non-répudiation: la *non-répudiation avec preuve de remise*, qui sert à rejeter toute fausse déclaration d'un destinataire qui nie avoir reçu des données, et la *non-répudiation avec preuve d'origine*, qui sert à rejeter toute fausse déclaration d'un expéditeur qui nie avoir envoyé des données. Toutefois, dans un sens plus général, le concept de non-répudiation peut être appliqué à de nombreux contextes différents, notamment la non-répudiation de création, de soumission, de stockage, de transmission et de réception de données. La Recommandation UIT-T X.813 élargit les concepts des services de sécurité de non-répudiation décrits dans la Recommandation UIT-T X.800 et sert de cadre pour la définition de ces services. En outre, elle définit différents mécanismes de prise en charge de ces services et les exigences générales de gestion concernant la non-répudiation.

La *confidentialité* est la propriété d'une information qui n'est ni communiquée, ni divulguée aux individus, entités ou processus non autorisés. Le service de confidentialité a pour objet de protéger les informations contre toute divulgation non autorisée. La confidentialité des informations fait l'objet de la Recommandation UIT-T X.814, qui définit les concepts de base de la confidentialité, différentes classes de confidentialité et les fonctionnalités requises pour chaque classe de mécanismes de confidentialité. Elle définit également les services de gestion et les services support requis ainsi que l'interaction avec les autres services et mécanismes de sécurité.

L'*intégrité des données* est la propriété de données qui n'ont pas été modifiées de façon non autorisée. En général, un service d'intégrité répond à la nécessité de garantir que les données ne sont pas corrompues ou, si elles le sont, que l'utilisateur est au courant de cette corruption. La Recommandation UIT-T X.815 porte sur l'intégrité des données au moment de leur extraction, de leur transfert et de leur gestion. Elle définit les concepts de base de l'intégrité, différentes classes de mécanismes d'intégrité et les fonctionnalités, exigences de gestion et services connexes nécessaires pour chaque classe de mécanismes. (Il est à noter que, bien que les normes sur les architectures de sécurité portent essentiellement sur l'intégrité des données, d'autres aspects de l'intégrité, par exemple l'intégrité des systèmes, sont également importants pour la sécurité.)

4.3 Architecture de sécurité pour les systèmes assurant des communications de bout en bout

En 2003, après un examen approfondi de l'architecture de sécurité pour les réseaux, la Recommandation UIT-T X.805 a été approuvée. Cette architecture, qui reprend et élargit certains concepts de la Recommandation UIT-T X.800 ainsi que les cadres de sécurité présentés ci-dessus, peut être appliquée à divers types de réseau et ne dépend pas de la technologie.

4.3.1 Eléments de l'architecture définie dans la Recommandation UIT-T X.805

L'architecture décrite dans la Recommandation UIT-T X.805 est définie sur la base de trois principaux concepts pour les réseaux de bout en bout: les couches, les plans et les dimensions de sécurité. On adopte une approche hiérarchique de subdivision des exigences de sécurité entre les couches et les plans de manière à assurer la sécurité de bout en bout en définissant des mesures de sécurité dans chacune des dimensions pour prendre en compte les menaces spécifiques. La Figure 1 illustre les éléments de cette architecture.

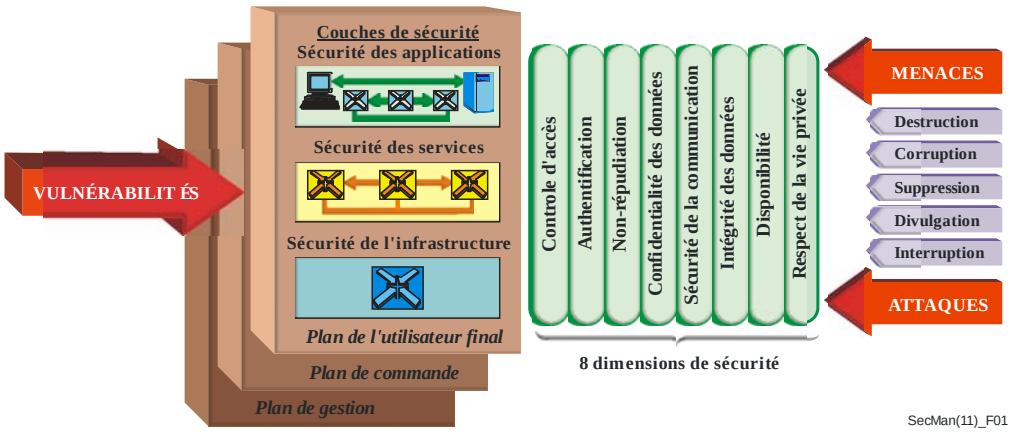


Figure 1 – Eléments de l'architecture de sécurité de la Recommandation UIT-T X.805

Une *dimension de sécurité* est un ensemble de mesures de sécurité destiné à couvrir un aspect particulier de la sécurité du réseau. Les services de sécurité de base décrits dans la Recommandation UIT-T X.800 (*Contrôle d'accès, authentification, confidentialité des données, intégrité des données* et *non-répudiation*) se retrouvent dans les fonctionnalités des *dimensions de sécurité* correspondantes de la Recommandation UIT-T X.805 (illustrées sur la Figure 1). En outre, la Recommandation UIT-T X.805 introduit trois dimensions (*Sécurité de la communication, disponibilité* et *respect de la vie privée*) qui ne figurent pas dans la Recommandation UIT-T X.800:

- la dimension *sécurité de la communication*, qui permet de faire en sorte que les informations circulent uniquement entre les points d'extrémité autorisés, c'est-à-dire qu'elles ne sont ni déviées ni interceptées le long de leur trajet entre ces points d'extrémité;

- la dimension *disponibilité*, qui permet de garantir qu'il n'y a pas déni de l'accès autorisé aux éléments de réseau, aux informations stockées, aux flux d'informations, aux services et aux applications en raison d'événements ayant une incidence sur le réseau; et

- la dimension *respect de la vie privée*, qui permet d'assurer la protection des informations qui pourraient être obtenues à partir de l'observation des activités dans le réseau. On peut citer par exemple les sites web qu'un utilisateur a visités, l'emplacement géographique d'un utilisateur, ainsi que les adresses IP et les noms DNS des dispositifs présents dans le réseau d'un fournisseur de services.

Ces dimensions offrent une protection de réseau complémentaire contre toutes les principales menaces de sécurité. Elles ne sont pas limitées au réseau mais couvrent aussi les applications et les informations des utilisateurs finals. Les dimensions de sécurité s'appliquent aux fournisseurs de service ou entreprises qui offrent des services de sécurité à leurs clients.

Afin de disposer d'une solution de sécurité de bout en bout, les dimensions de sécurité doivent être appliquées à une hiérarchie de groupes d'équipements et d'installations de réseau, qu'on désigne comme étant les *couches de sécurité*. Un *plan de sécurité* représente un certain type d'activité dans le réseau, protégée par des dimensions de sécurité. Chaque plan de sécurité représente un type d'activité protégée dans le réseau.

Les couches de sécurité définissent les exigences qui s'appliquent aux éléments de réseau et aux systèmes ainsi qu'aux services et applications associés à ces éléments. La définition des 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. Les trois couches sont les suivantes:

- la couche *infrastructure*, qui représente les modules fondamentaux des réseaux, de leurs services et de leurs applications. Parmi les composants qui appartiennent à cette couche figurent notamment les différents éléments de réseau, en particulier les routeurs, les commutateurs et les serveurs, ainsi que les liaisons de communication qui les relient;

- la couche *services*, qui définit 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; et

- la couche *applications*, qui définit les exigences relatives aux applications de réseau utilisées par les clients. Ces applications peuvent être aussi simples que la messagerie électronique ou aussi complexes que, par exemple, la visualisation collaborative, pour laquelle des transferts vidéo haute définition sont opérés dans des domaines comme ceux de l'exploration pétrolière ou de la conception d'automobiles.

Les plans de sécurité 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. Les réseaux devraient être conçus de manière à ce que les événements se produisant sur un plan de sécurité soient isolés des autres plans de sécurité.

Les plans de sécurité sont les suivants:

- le plan de *gestion*, qui se rapporte aux activités d'exploitation, d'administration, de maintenance et de configuration, par exemple la configuration d'un utilisateur ou d'un réseau;

- le plan de *commande*, qui est associé aux aspects de signalisation pour l'établissement (et la modification) de la communication de bout en bout dans le réseau, quels que soient le support ou la technologie utilisés dans le réseau; et

- le plan d'*utilisateur final*, dans lequel il s'agit d'assurer la sécurité d'accès au réseau et d'utilisation du réseau par les abonnés. Il s'agit aussi d'assurer la protection des flux de données d'utilisateur final.

L'architecture définie dans la Recommandation UIT-T X.805 peut servir de guide pour élaborer des politiques de sécurité, des architectures techniques et des plans d'intervention en cas d'incident et de retour à la normale. Elle peut aussi servir de base à une évaluation de la sécurité. Dès qu'un programme de sécurité a été mis en place, il doit être tenu à jour compte tenu de l'évolution permanente de l'environnement des menaces. Cette architecture de sécurité peut faciliter la tenue à jour d'un programme de sécurité, en permettant de veiller à ce que les modifications apportées au programme prennent en considération les dimensions de sécurité applicables dans chaque couche et chaque plan de sécurité.

La Recommandation UIT-T X.805 porte sur une architecture de sécurité pour les réseaux, mais certains concepts peuvent être élargis aux dispositifs d'utilisateur final. Cet aspect est pris en compte dans la Recommandation UIT-T X.1031.

4.3.2 Disponibilité du réseau et de ses composants

La disponibilité du réseau est un aspect important de la sécurité des TIC. Comme indiqué plus haut, la dimension de sécurité *disponibilité* de la Recommandation UIT-T X.805 a pour objet de garantir la continuité de service et de garantir l'accès aux éléments de réseau, aux informations et aux applications lorsque cet accès est autorisé. Les solutions de retour à la normale après une catastrophe sont comprises dans cette dimension.

Les exigences fonctionnelles et opérationnelles destinées à limiter les risques d'indisponibilité des ressources de réseau et d'en réduire les conséquences sont nombreuses et variées. Parmi les nombreux facteurs à prendre en considération, on peut citer les caractéristiques d'erreurs, la limitation des encombrements, la signalisation des défaillances et les mesures correctives. La Recommandation UIT-T G.827 définit les paramètres et objectifs de disponibilité pour les conduits numériques internationaux de bout en bout à débit constant ou des éléments de ces conduits. Ces paramètres sont indépendants du type de réseau physique prenant en charge le conduit de bout en bout. L'Annexe A de la Recommandation UIT-T G.827 donne des indications détaillées sur les méthodes permettant d'évaluer la disponibilité de bout en bout et donne des exemples de topologies de conduit et de calculs de disponibilité de conduit de bout en bout. D'autres Recommandations traitent de la qualité de fonctionnement des réseaux, notamment les Recommandations UIT-T G.1000, UIT-T G.1030, UIT-T G.1050 et UIT-T G.1081.

4.4 Guide de mise en œuvre

Les normes de l'UIT-T sur l'architecture de sécurité appartiennent toutes à la série de Recommandations UIT-T X.800-849 sur la sécurité. Un guide de mise en œuvre est fourni dans le Supplément 3 aux Recommandations UIT-T de la série X. Ce supplément énonce des lignes directrices concernant les activités critiques pendant le cycle de vie de la sécurité dans les réseaux. Quatre domaines sont traités: politique de sécurité technique; identification des actifs hiérarchiques; menaces, vulnérabilités et solutions d'atténuation en fonction des actifs hiérarchiques; et évaluation de la sécurité. Les lignes directrices et les tableaux associés visent à permettre de mettre en place de façon systématique une planification, une analyse et une évaluation de la sécurité dans les réseaux.

4.5 Architectures propres à certaines applications

Le présent paragraphe expose certains aspects des architectures applicables à certaines applications.

4.5.1 Communications entre homologues

Dans un réseau entre homologues (P2P), tous les homologues ont une autorité et des attributions équivalentes. Contrairement à ce qui passe dans le cas du modèle client/serveur, un homologue communique directement avec d'autres homologues lors de l'échange de données ou de messages. Etant donné que le trafic et le traitement sont l'affaire de chaque homologue, le réseau P2P n'a pas besoin d'une grande performance en termes de puissance de traitement ou d'une grande largeur de bande.

Le réseau P2P est superposé sur le réseau de télécommunication et l'Internet. Il s'appuie non pas sur des ressources centralisées classiques mais sur la connectivité entre les nœuds et sur la puissance de traitement et la capacité de stockage disponibles dans chaque nœud.

Les réseaux P2P servent généralement à raccorder des nœuds au moyen de connexions ad hoc. D'utilisations diverses, ces réseaux assurent par exemple le partage de fichiers de données numériques, notamment de fichiers audio, vidéo et texte. La technologie P2P est également utilisée pour des communications en temps réel (téléphonie par exemple).

4.5.1.1 Architecture de sécurité et opérations pour les réseaux entre homologues

Une architecture générale relative à la sécurité qui peut être appliquée dans divers réseaux P2P est décrite dans la Recommandation UIT-T X.1162.

La Figure 2 illustre une architecture de service P2P de base. Les informations traitées par chaque homologue sont échangées directement entre les utilisateurs. Comme il n'existe pas de serveur central pour le stockage des informations, chaque homologue doit trouver quels homologues possèdent les données cibles avant de pouvoir récupérer ces données. De plus, chaque homologue doit permettre aux autres homologues d'accéder à ses données avant que l'échange de données puisse avoir lieu.

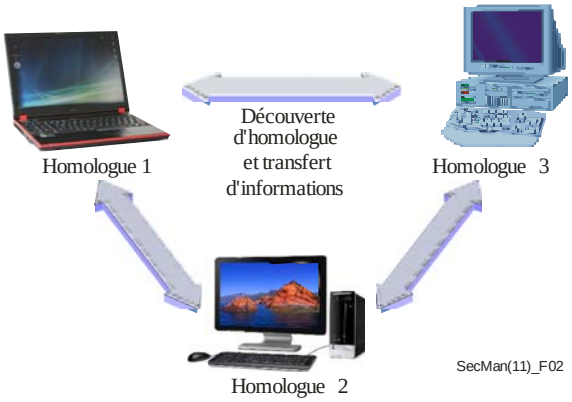


Figure 2 – Architecture de service P2P

Dans le réseau P2P physique, un utilisateur peut accéder aux services P2P au moyen d'un dispositif. Le terme "homologue" désigne généralement un utilisateur ou un dispositif de l'utilisateur. On distingue les types suivants de connexion entre les entités dans un réseau P2P:

- connexion avec un homologue intradomaine;
- connexion avec un homologue interdomaines; et
- connexion avec un fournisseur de service homologue situé dans un autre domaine de réseau.

La Figure 3 illustre l'architecture de réseau P2P logique en tant que réseau virtuel sur la strate de transport. On part du principe que le fonctionnement de chaque homologue n'est pas limité par l'architecture de réseau physique et qu'un homologue peut communiquer avec n'importe quel autre homologue quel que soit son emplacement (avec l'aide d'un super-homologue, si nécessaire). La structure du réseau entre homologues est subdivisée en deux strates: la strate de superposition P2P et la strate de transport. La strate de transport est chargée du transfert des paquets en provenance ou à destination de la couche supérieure et la strate de superposition est chargée de la fourniture des services P2P.

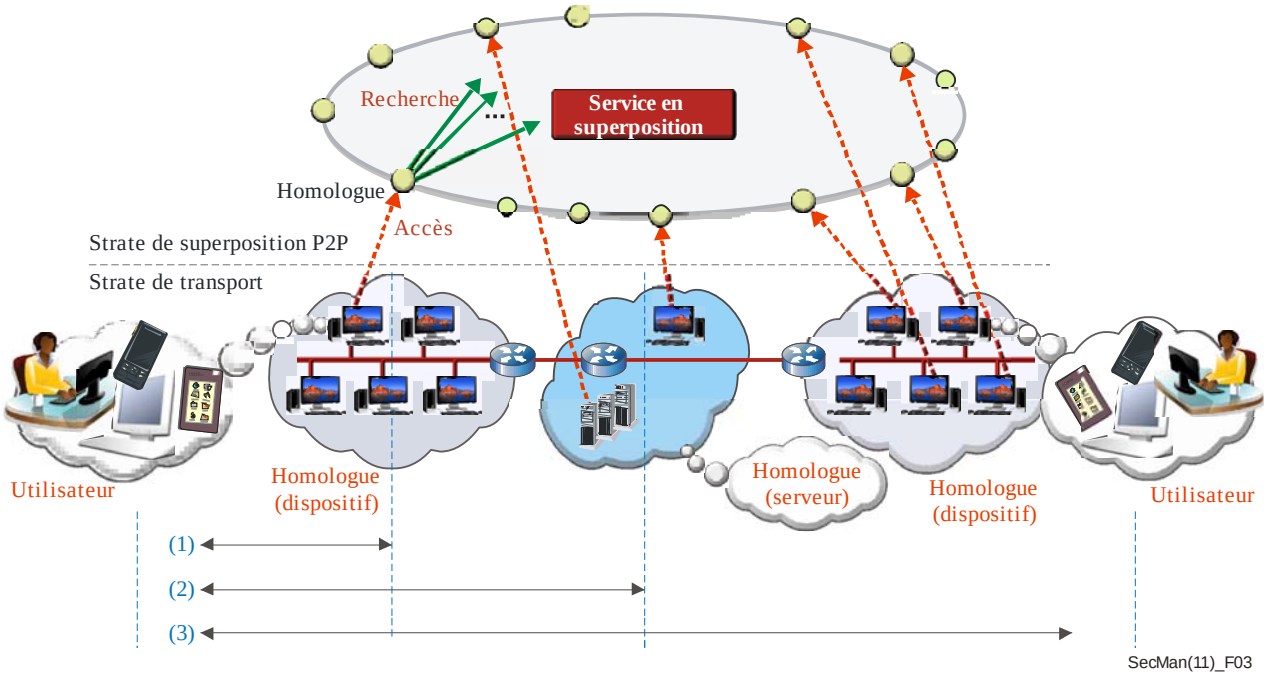


Figure 3 – Modèle de référence de l'architecture du réseau P2P

4.5.1.2 Cadre général des communications sécurisées entre homologues

Les exigences de sécurité pour les réseaux P2P ainsi que les services et mécanismes nécessaires pour satisfaire ces exigences font l'objet de la Recommandation UIT-T X.1161.

Les menaces qui pèsent sur les communications P2P sont notamment les suivantes: écoute clandestine, brouillage, injection & modification, accès non autorisé, répudiation, attaques de l'intercepteur (*man-in-the-middle*) et attaques Sybil. Les mesures permettant de lutter contre les menaces P2P sont indiquées dans le Tableau 3.

Tableau 3 – Relation entre les exigences de sécurité P2P et les contre-mesures

Contre-mesures / Exigences	Chiffrement	Echange de clés	Signature numérique	Gestion de la confiance	Contrôle d'accès	Mécanisme d'intégrité des données	Echange pour authentification	Notarisation	Routage sécurisé	Mécanisme de contrôle du trafic	Attribution d'un identifiant
Authentification de l'utilisateur	X	X	X	X	X		X				X
Anonymat	X			X							X
Respect de la vie privée	X				X		X				
Intégrité des données	X	X	X		X	X	X				
Confidentialité des données	X	X			X		X				
Contrôle d'accès					X		X				X
Non-répudiation			X				X	X			X
Utilisabilité					X						
Disponibilité					X		X		X	X	
Traçabilité			X						X		X
Contrôle du trafic		X								X	

4.5.2 Architecture de sécurité des messages dans l'environnement des services web mobiles

L'architecture de sécurité des messages dans l'environnement des services web mobiles et les scénarios associés sont décrits dans la Recommandation UIT-T X.1143. Cette norme définit:

- une architecture de sécurité des messages qui repose sur des mécanismes de politique de service web appropriés;
- des mécanismes d'interfonctionnement et des scénarios de service entre les applications qui prennent en charge toute la pile de protocoles de sécurité des services web et les applications existantes qui ne prennent pas en charge toute cette pile;
- des mécanismes d'authentification, d'intégrité et de confidentialité des messages;
- un mécanisme de filtrage des messages reposant sur leur contenu; et
- une architecture de sécurité des messages de référence et des scénarios pour les services de sécurité.

La Figure 4 illustre l'architecture de sécurité UIT-T X.1143 pour les services web mobiles.

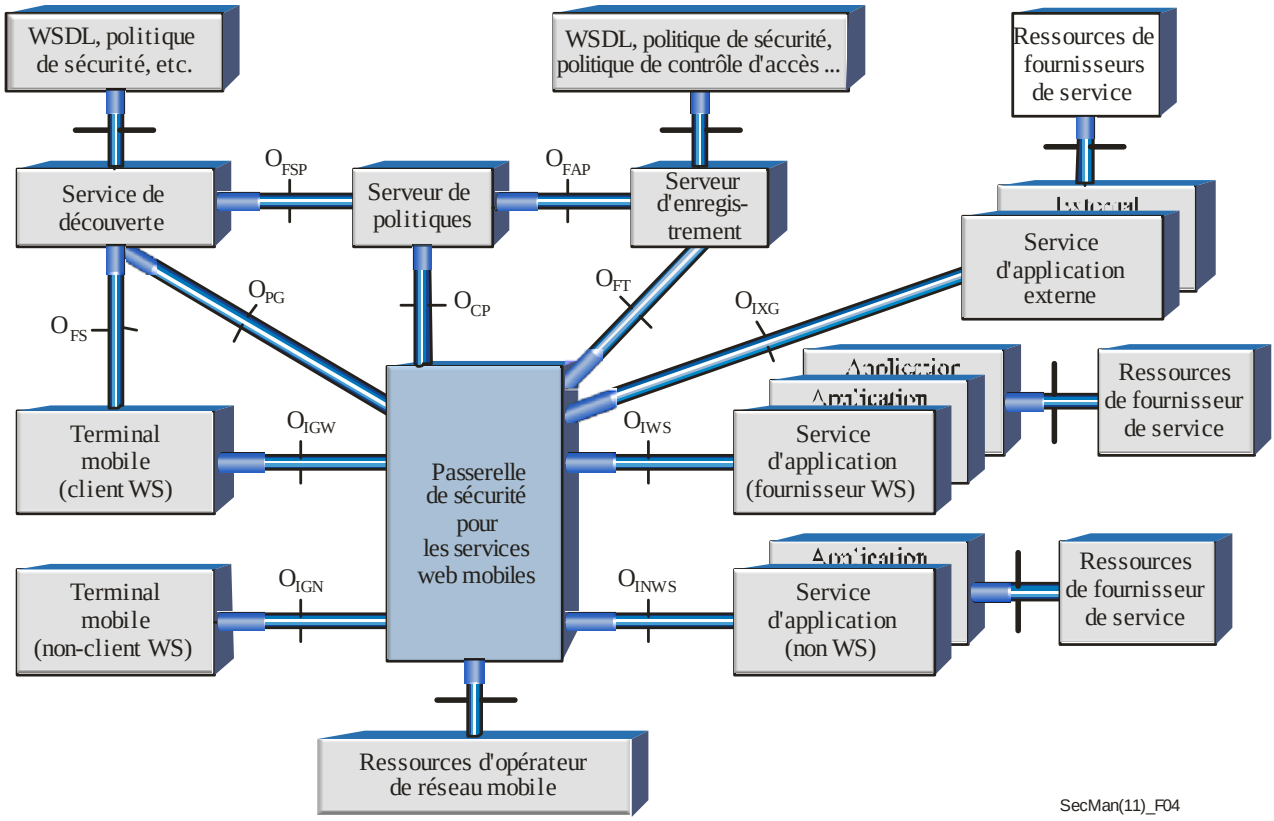


Figure 4 – Architecture de sécurité pour les services web mobiles

L'architecture de sécurité pour les services web mobiles comprend:

- des terminaux mobiles, qui sont des clients des services web mobiles;
- une passerelle de sécurité pour les services web mobiles (MWSSG). Toutes les demandes émanant de clients mobiles sont envoyées à la passerelle MWSSG, qui applique un contrôle d'accès;
- le serveur de politiques, qui gère les politiques de sécurité relatives au traitement sécurisé des messages et les politiques de contrôle d'accès aux messages;
- le service d'application, qui offre divers services à valeur ajoutée aux clients;
- le service de découverte, qui stocke les informations d'interface pour les services d'application et les politiques de sécurité associées pour l'accès aux services d'application par les clients; et
- le serveur d'enregistrement, qui réside dans le domaine interne de l'opérateur mobile et gère les informations d'interface pour les services d'application, les politiques de sécurité associées pour l'accès aux services d'application par les clients et les politiques de contrôle d'accès relatives aux services cibles.

Un cadre de sécurité pour la mobilité dans la strate de transport des réseaux de prochaine génération (NGN) est défini dans la Recommandation UIT-T Y.2760, qui traite des exigences de sécurité, des mécanismes de sécurité et des procédures de gestion et de contrôle de la mobilité dans les réseaux NGN.

4.6 Architecture de corrélations externes

Les corrélations entre un système de sécurité d'un réseau de télécommunication (TNSS) IP et divers groupes d'objets externes sont décrites dans la Recommandation UIT-T X.1032. Cette norme traite des quatre types de corrélation externe suivants:

- corrélations d'un système TNSS avec les systèmes de sécurité de systèmes d'information et structure d'information;
- corrélations d'un système TNSS avec les objets d'un système de télécommunication;
- corrélations d'un système TNSS avec des organisations externes; et
- corrélations d'un système TNSS avec les sources de menace pour la sécurité.

La Figure 5, tirée de la Recommandation UIT-T X.1032, illustre les fonctions des objets externes et leur effet sur un système TNSS.

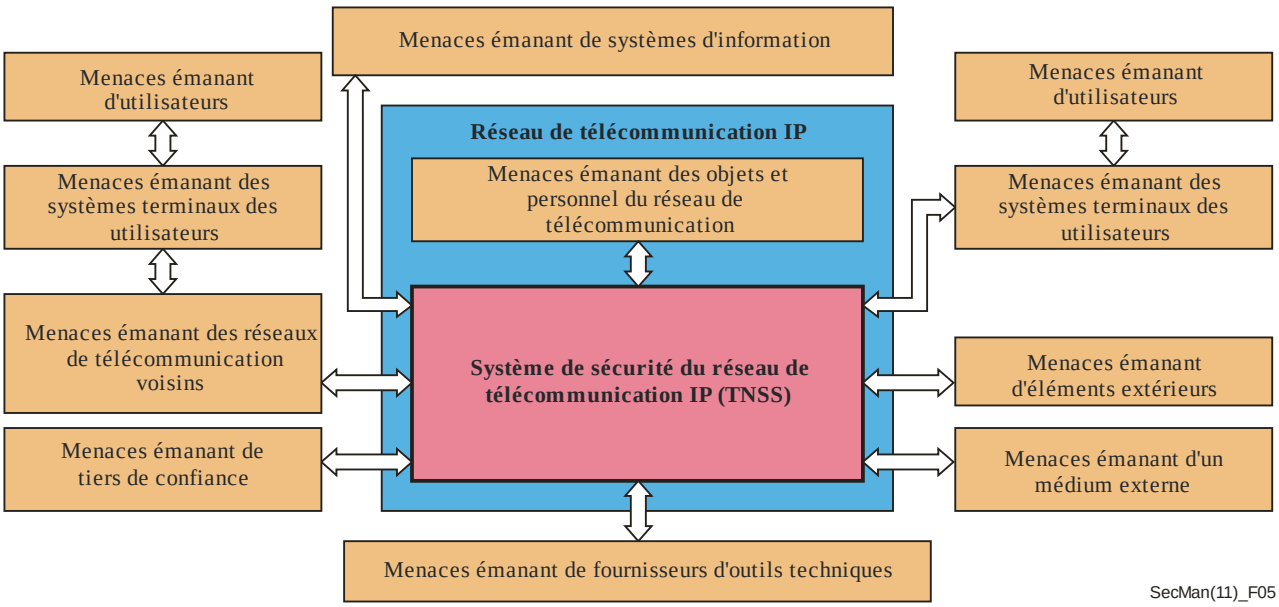


Figure 5 – Modèle de corrélations d'un système TNSS avec les sources de menace pour la sécurité

Les menaces sont classées en cinq types comme l'indiquent les Recommandations UIT-T X.800 et UIT-T X.805:

- destruction des informations et d'autres ressources;
- altération ou modification des informations;
- vol, suppression ou perte d'informations et d'autres ressources;
- divulgation d'informations; et

- interruption de services.

La politique de sécurité dans un réseau de télécommunication peut être utilisée pour riposter à toutes les menaces, ou à certaines de ces menaces. En conséquence, les dimensions de sécurité requises sont sélectionnées au cours de l'élaboration du système TNSS. Les corrélations externes d'un système TNSS avec les sources de menaces pour la sécurité peuvent faire intervenir:

- des interfaces électriques;
- des actions de personnes;
- des attaques utilisant des moyens techniques via le réseau de télécommunication et des moyens techniques externes;
- des influences de l'environnement externe;
- des mesures techniques de riposte aux attaques;
- des mesures organisationnelles de riposte aux attaques.

4.7 Autres architectures et modèles de sécurité de réseau

D'autres aspects des architectures de sécurité de réseau sont abordés plus loin dans le texte. On pourra en particulier se reporter aux paragraphes 7.2, Architecture de gestion de réseau; 8.1, Sécurité des réseaux de prochaine génération (NGN); 8.4.1, Architecture IPCablecom; et 10.2, TVIP.

5. Aspects de gestion de la sécurité

5 Aspects de gestion de la sécurité

La gestion de la sécurité est un vaste sujet qui englobe de nombreuses activités associées au contrôle et à la protection de l'accès aux ressources des systèmes et des réseaux, à la surveillance des événements, à la notification, aux politiques et à l'audit, ainsi qu'à la gestion des informations relatives à ces fonctions et activités. Le présent Chapitre porte sur certaines activités génériques de gestion de la sécurité. Les activités de gestion de la sécurité associées à la sécurisation de l'infrastructure de réseau sont examinées dans le Chapitre 7.

5.1 Gestion de la sécurité des informations

Tout comme les autres actifs, les informations sont essentielles pour les activités d'une organisation. Elles peuvent être imprimées, stockées sous forme électronique, transmises par courrier, communiquées par voie électronique, affichées dans des films, communiquées dans des conversations ou acheminées par d'autres moyens. Quelle que soit leur forme ou leur fonctionnalité, ou le moyen utilisé pour les partager ou les stocker, les informations devraient toujours bénéficier d'une protection appropriée.

Les organisations dont les installations sont utilisées par les abonnés pour le traitement d'informations (données personnelles, données confidentielles, données sensibles, etc.) doivent garantir un niveau de protection approprié pour empêcher toute compromission des informations, autrement dit, elles doivent établir un système de gestion de la sécurité des informations (ISMS) efficace.

En cas de violation de la sécurité des informations, par exemple en cas d'accès non autorisé au système de traitement de l'information d'une organisation, cette dernière peut subir des dommages importants. Il est donc essentiel pour une organisation de protéger ses informations efficacement en mettant en place un processus structuré de gestion de la sécurité et, en particulier, en mettant en place et en appliquant un ensemble de contrôles appropriés. Ces contrôles, qui s'appliquent aux données, installations de télécommunication, services et applications, doivent être établis, appliqués, surveillés, revus et améliorés en permanence. L'absence de déploiement de contrôles de sécurité efficaces peut empêcher une organisation de remplir ses objectifs de sécurité et les objectifs propres à ses activités.

La spécification ISMS la plus largement reconnue est celle qui est définie dans la série de normes ISO/CEI 27000 qui contient des normes sur les fondements du système ISMS, les exigences, un code de bonne pratique, un guide de mise en œuvre et des aspects connexes. L'UIT-T et l'ISO/CEI ont élaboré conjointement la Recommandation UIT-T X.1051 | Norme internationale ISO/CEI 27011, sur la base de la norme ISO/CEI 27002 (Code de bonne pratique pour la gestion de la sécurité des informations).

La Recommandation UIT-T X.1051 établit des lignes directrices et des principes généraux pour instaurer, mettre en œuvre, maintenir et améliorer la gestion de la sécurité des informations dans les organisations de télécommunication et donne des indications de base pour la mise en œuvre de la gestion de la sécurité des informations afin de contribuer à garantir la confidentialité, l'intégrité et la disponibilité des installations et services de télécommunication. Des indications destinées tout particulièrement au secteur des télécommunications sont données sur les aspects suivants:

- organisation de la sécurité des informations;
- gestion des actifs;
- sécurité des ressources humaines;
- sécurité physique et environnementale;
- gestion des communications et gestion de l'exploitation;

- contrôle d'accès;
- acquisition de systèmes d'information;
- développement et maintenance;
- gestion des incidents; et
- gestion de la continuité des activités.

En plus de l'application des objectifs et contrôles de sécurité décrits dans la Recommandation UIT-T X.1051, les organisations de télécommunication doivent aussi tenir compte de ce qui suit:

- les informations doivent être protégées contre toute divulgation non autorisée. Ainsi, l'existence, le contenu, l'origine, la destination et les date et heure des informations communiquées ne doivent pas être divulguées;
- la mise en place et l'utilisation des installations de télécommunication devraient être contrôlées afin de garantir l'authenticité, l'exactitude et l'exhaustivité des informations transmises, relayées ou reçues par câble, par voie hertzienne ou par toute autre méthode; et
- tout accès à des informations et installations et au support utilisé pour la fourniture de services de communication doit être autorisé et ne devrait être accordé que lorsque c'est nécessaire. Dans le prolongement des dispositions relatives à la disponibilité, les organisations devraient donner la priorité aux communications essentielles en cas d'urgence et devraient se conformer aux réglementations applicables.

Afin de réduire les risques, une mise en œuvre correcte de la gestion de la sécurité des informations est nécessaire dans les organisations de télécommunication, quel que soit le support ou le mode de transmission.

Pour la fourniture de leurs services, les organisations de télécommunication font office d'intermédiaire dans le transfert des données opéré par d'autres organisations ou par des particuliers. Il faut donc tenir compte du fait que les installations de traitement de l'information d'une organisation sont accessibles et utilisées non seulement par ses propres employés et contractuels, mais aussi par divers utilisateurs en dehors de l'organisation.

Sachant que les services et installations de télécommunication peuvent être utilisés en partage et/ou faire l'objet d'une interconnexion avec d'autres fournisseurs de services, l'infrastructure de réseau, les services, les applications et les installations doivent absolument tous être pris en compte pour la gestion de la sécurité des informations dans les organisations de télécommunication.

5.2 Cadre de gestion de la sécurité de l'information

La Recommandation UIT-T X.1051 définit les catégories de contrôles de sécurité pour les télécommunications. La Recommandation UIT-T X.1052 présente plusieurs des activités principales consistant à diriger la mise en œuvre des contrôles de sécurité et à fournir une assistance en la matière, et associe en outre les contrôles spécifiés dans la Recommandation UIT-T X.1051 et d'autres Recommandations qui contiennent des lignes directrices propres à un certain nombre de domaines de gestion de la sécurité de l'information, telles que les Recommandations UIT-T X.1055, UIT-T X.1056 et UIT-T X.1057, comme indiqué dans la Figure 6.

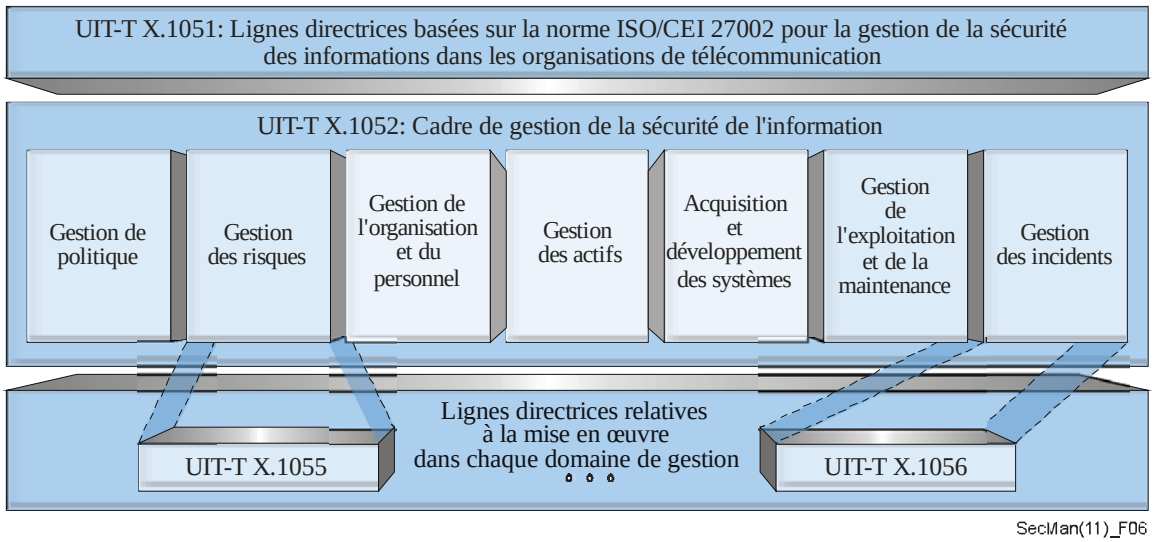


Figure 6 – Relation entre la Recommandation UIT-T X.1052 et les autres Recommandations concernant la gestion de la sécurité de l'information

Il est nécessaire que les organisations de télécommunication confirment la portée de leur système ISMS, lequel comprend les actifs liés à l'information. Cette confirmation, ainsi que l'établissement de lignes directrices relatives à la mise en œuvre de la gestion de la sécurité de l'information, devraient précéder l'évaluation des risques pesant sur les actifs liés à l'information et le contrôle ultérieurs de ces risques. En outre, il est nécessaire de définir la structure et la forme de l'organisation de la sécurité de l'information, lesquelles serviront de base pour le contrôle des risques liés à la mise en œuvre. Les activités de contrôle des risques menées par les organisations ne devraient pas être dissociées du fonctionnement de celles-ci. Le fonctionnement d'une organisation est généralement décrit dans une série de procédures et il conviendrait que les activités de contrôle des risques fassent partie intégrante des procédures correspondantes.

Dans le cadre de gestion de la sécurité de l'information, les activités principales liées à la gestion de la sécurité de l'information dans le domaine des télécommunications sont envisagées sous trois angles:

a) encourager l'organisation à mettre en œuvre la gestion de la sécurité de l'information, y compris dans des domaines tels que la gestion de l'organisation et du personnel et la gestion des actifs;

b) mettre en place et améliorer de façon constante le système ISMS, y compris dans des domaines tels que la gestion des risques et la gestion de politique; et

c) mener des activités opérationnelles spécifiques, y compris dans des domaines tels que la gestion de l'acquisition et du développement des systèmes, la gestion de l'exploitation et de la maintenance et la gestion des incidents.

5.3 Gestion des risques

Par gestion des risques, on entend l'évaluation et la quantification des risques et la prise de mesures pour faire en sorte que les risques résiduels soient inférieurs à un niveau acceptable déterminé à l'avance. Ce sujet est présenté dans la Recommandation UIT-T X.1205. Des lignes directrices plus détaillées concernant la gestion des risques sont énoncées dans la Recommandation UIT-T X.1055, qui décrit des processus et des techniques pouvant être utilisés pour évaluer les exigences de sécurité des télécommunications et les risques associés et pour faciliter le choix, la mise en œuvre et la mise à jour de contrôles appropriés pour maintenir le niveau de sécurité requis.

Il existe un certain nombre de méthodes de gestion des risques. La Recommandation UIT-T X.1055 énonce les critères à utiliser pour évaluer et choisir des méthodes appropriées pour une organisation de télécommunication. Cependant, elle ne propose pas de méthode spécifique de gestion des risques.

Le processus de gestion des risques est illustré sur la Figure 7.

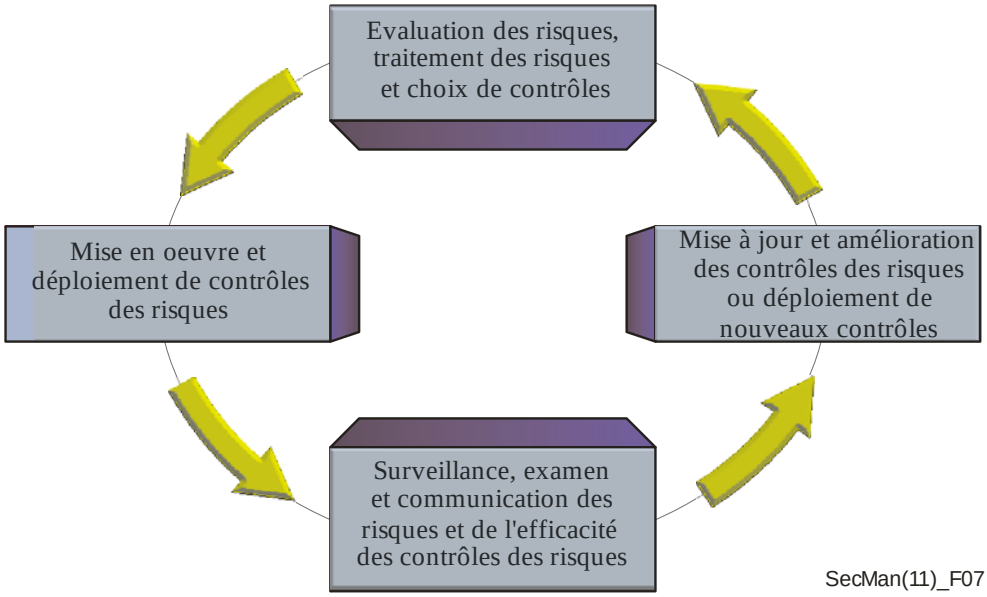


Figure 7 – Processus de gestion des risques (UIT-T X.1055)

Des profils de risques sont utilisés pour guider le processus global de gestion des risques. Plus précisément, ils sont utilisés pour faciliter la prise de décision et le classement des risques par ordre de priorité selon leur caractère critique et pour aider à déterminer l'attribution des ressources et les contre-mesures. Ils peuvent aussi être utiles pour élaborer des paramètres appropriés et être utilisés avec d'autres outils (méthodes d'analyse d'écart par exemple). La Recommandation UIT-T X.1055 donne des indications pour définir des profils de risques et contient un modèle de profil ainsi que quelques exemples de profils de risques.

5.4 Gestion des actifs

Un actif est un élément ou une entité auxquels l'organisation attribue directement une valeur. Les actifs d'une organisation ont une valeur unique qui leur est propre, du point de vue des activités de l'organisation, des affaires financières, de la fiabilité, etc. On peut considérer que la valeur des systèmes d'information et de communication relevant du système ISMS est supérieure à celles d'autres actifs. Les incidents qui concernent ces actifs peuvent avoir des conséquences négatives non seulement pour les utilisateurs, mais aussi pour les activités de l'organisation. Par conséquent, la protection de ces actifs doit être considérée comme étant hautement prioritaire. La plupart des organisations s'efforcent de trouver les meilleures méthodes pour identifier les actifs dont la protection est hautement prioritaire. L'objectif de la gestion des actifs est de recenser et de protéger les éléments les plus importants de l'organisation afin de minimiser le risque de problèmes. Pour déterminer l'importance des actifs, il convient de prendre en considération les services principaux et la valeur des activités, eu égard:

- à l'incidence potentielle sur les services et à l'éventail des services dans lesquels chaque actif intervient;
- au manque à gagner potentiel et au niveau des pertes financières potentielles;

- aux conséquences potentielles liées à la perte de clients; et
- à la détérioration potentielle de l'image de l'organisation.

Les organisations de télécommunication devraient se fixer des objectifs particulièrement élevés en ce qui concerne l'exploitation et la gestion de leurs divers actifs, la fourniture de services aux clients et l'appui direct ou indirect à leurs activités. Afin de protéger ces actifs, il est indispensable que les organisations de télécommunication veillent à ce que leurs activités et leurs services ne soient pas compromis.

La Recommandation UIT-T X.1057 donne un aperçu des procédures et des méthodes qu'il est nécessaire de mettre en place pour recenser, classer, évaluer et conserver les actifs qui appartiennent aux organisations de télécommunication.

Du point de vue de la sécurité de l'information, la gestion des actifs consiste à appliquer les mesures appropriées de traitement et de protection en fonction de la valeur des actifs, telle qu'elle est déterminée par l'organisation. Afin de gérer les différents actifs d'une organisation de façon systématique et sécurisée, il convient d'adopter un processus de gestion des actifs tout au long de leur durée de vie, qui couvre l'acquisition ou la création, la modification, et l'élimination ou la destruction de l'actif, conformément à des règles et normes prédéterminées. Le processus de gestion des actifs est illustré sur la Figure 8.

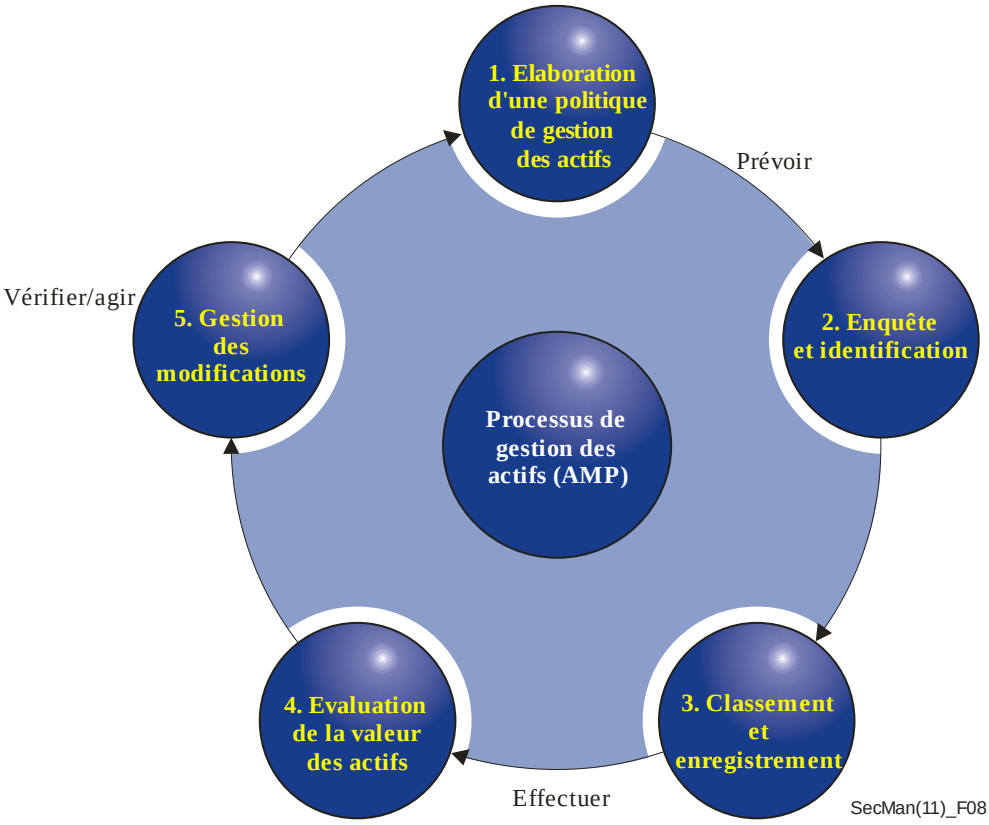


Figure 8 – Processus de gestion des actifs

La Recommandation UIT-T X.1057 contient des lignes directrices relatives aux activités détaillées propres à chaque processus, à savoir: élaboration d'une politique de gestion des actifs, enquête et identification, classement et enregistrement, évaluation de la valeur des actifs et gestion des modifications. Cette Recommandation présente également les actifs propres aux télécommunications à l'aide des exemples figurant dans le Tableau 4.

Tableau 4 – Exemples d'actifs en général et d'actifs propres aux télécommunications

Type d'actif	Description	Exemples	
		Propres aux télécommunications	Général
Informations électroniques	Informations stockées sous forme électronique	Informations relatives aux clients des services de télécommunication (base de données), journal des sessions du réseau et des accès au réseau, fichiers de configuration du réseau, politiques d'utilisation des services et d'accès aux services, etc.	Base de données (BD de bureau, etc.), fichiers de données (politiques et lignes directrices de bureau, journal d'un système de télévision en circuit fermé, etc.), fichiers système (fichiers de configuration, fichiers de journalisation, etc.), etc.
Document papier	Informations sur un support papier, à savoir des documents ou des dossiers produits ou utilisés au cours des activités	Contrats et accords, y compris les SLA, diagramme de l'architecture de réseau, liste des adresses IP, schéma de câblage, diagramme du système serveur, manuels des systèmes d'exploitation de réseau, etc.	Contrats et accords, documents de système (diagramme de configuration du réseau, manuel d'utilisation, etc.), etc.
Logiciel	Logiciel développé à des fins commerciales ou pour l'organisation elle-même	Système d'exploitation de réseau, scanner réseau, outils et systèmes de détection d'alerte avancée, logiciel d'enregistrement d'audit, etc.	Logiciel d'application (application de bureau, etc.) , logiciel système (OS, DBMS, scanner de vulnérabilités, etc.), outils et systèmes de développement, etc.
Matériel	Serveur et dispositifs de réseau utilisés pour les services ou activités internes et externes	Serveur (serveur DNS, serveur DHCP, serveur de journalisation, serveur d'authentification, serveur NTP, serveur NMS, serveur de supervision, etc.), équipements de réseau et de communications (router dorsal, commutateur, CMTS, NAS/RAS, AP, modem, etc.), équipements de sécurité (ESM, pare-feu, IPS, IDS, VPN, VirusWall, antivirus, etc.), systèmes mobiles, systèmes à satellites (stations), systèmes à hyperfréquences, système de transmission, etc.	Serveur (serveur web, serveur BD, WAS, serveur de journalisation, serveur de sauvegarde, stockage, etc.), ordinateurs centraux, équipements de réseau et de communications (commutateur, etc.), équipements de sécurité, ordinateurs de bureaux, postes de travail, ordinateurs portables, équipements portatifs, etc.

Type d'actif	Description	Exemples	
		Propres aux télécommunications	Général
Installation	Lieux où les systèmes sont installés et exploités, qui englobent des espaces physiques et les salles des différents équipements d'appui	Installations de câblage, installations consacrées à la gestion et à la surveillance du réseau, salle des équipements de télécommunication, centre de données Internet, etc.	Immeuble de bureaux, salle des serveurs, salle des documents, salle des équipements électriques, etc.
Systèmes et équipements d'appui	Equipements utilisés pour la prise en charge de l'exploitation des systèmes d'information, tels que les équipements d'alimentation électrique, de climatisation, etc.	Systèmes d'appui pour les réseaux mobile, fixe et à satellites (générateur, UPS, etc.), etc.	Equipements électriques, équipements de climatisation, équipements d'extinction d'incendie, système de télévision en circuit fermé, etc.

6. Authentification et rôle de l'annuaire

6 Authentification et rôle de l'annuaire

L'authentification est un service de sécurité de plus en plus important, qui repose, dans une large mesure, sur les services d'annuaire. Outre l'authentification, l'annuaire prend en charge un certain nombre d'autres services essentiels de sécurité et certains des mécanismes utilisés pour fournir ces services, en particulier les services cryptographiques.

Le terme anglais "directory" désigne généralement un répertoire, autrement dit un ensemble organisé d'informations ou de fichiers qui peuvent être interrogés pour obtenir des informations particulières. Au sein de l'UIT-T et, plus généralement, dans le cadre de la normalisation de la sécurité et des télécommunications, le terme anglais "directory" désigne un *annuaire*, autrement dit un répertoire d'informations reposant sur la série de Recommandations UIT-T X.500, qui ont été élaborées conjointement avec l'ISO/CEI. L'annuaire, qui est présenté dans la Recommandation UIT-T X.500, et décrit en détail dans les Recommandations UIT-T X.501, UIT-T X.509, et UIT-T X.519, fournit des services d'annuaire pour faciliter les communications et l'échange d'informations entre des entités, des personnes, des terminaux, des listes de distribution, etc. Les services d'annuaire classiques sont notamment les suivants: nommage, correspondance nom-adresse, établissement d'un lien entre les objets et leur emplacement. Mais l'annuaire joue aussi un rôle important dans la prise en charge des services de sécurité par la définition et la conservation de justificatifs d'authentification sous la forme de certificats de sécurité. En particulier, la série de Recommandations UIT-T X.500 porte sur deux aspects de la sécurité:

- la protection des informations d'annuaire, définie essentiellement dans les Recommandations UIT-T X.501 et UIT-T X.509; et
- les principes de base de l'infrastructure de clé publique (PKI) et de l'infrastructure de gestion de privilège (PMI), définis dans la Recommandation UIT-T X.509.

Dans le présent chapitre, on commence par examiner l'importance que revêt la sécurité de l'annuaire proprement dit et la nécessité de protéger les informations de l'annuaire. On s'intéresse ensuite au rôle de l'annuaire dans la prise en charge de l'authentification forte, des infrastructures de clé publique, de la gestion d'identité et de la télébiométrie.

6.1 Protection des informations de l'annuaire

6.1.1 Objectifs de protection de l'annuaire

La protection des données de l'annuaire est essentiellement une question de respect de la vie privée (à savoir éviter la divulgation non autorisée d'informations personnelles sensibles), mais elle implique également de garantir l'intégrité des données et de protéger les actifs représentés par les données.

Un annuaire contient des informations sur des entités. Ces informations peuvent être sensibles et ne devraient être communiquées qu'à ceux qui ont à la fois le *droit de savoir* et *besoin de savoir*.

On distingue trois aspects de la protection des données:

- authentification de l'utilisateur qui cherche à accéder aux informations;
- contrôle d'accès afin de protéger les données contre tout accès non autorisé (Note – Une authentification correcte est nécessaire pour le contrôle d'accès.); et
- protection de la confidentialité des données, pour laquelle un contrôle d'accès correct est nécessaire.

Les caractéristiques de protection de la confidentialité des données ont toujours constitué une partie essentielle de la Recommandation UIT-T X.500, qui est la seule spécification d'annuaire à décrire ces caractéristiques importantes.

6.1.2 Authentification des utilisateurs de l'annuaire

Un annuaire UIT-T X.500 peut autoriser l'accès anonyme à certaines de ses informations non sensibles. Cependant, pour accéder à des données plus sensibles, un certain niveau d'authentification des utilisateurs est nécessaire. Dans la Recommandation UIT-T X.500, quatre niveaux d'authentification sont définis, à savoir:

a) nom uniquement;

b) nom et mot de passe non protégé: le mot de passe est transmis en clair sur la connexion (lequel, lorsqu'on utilise la pile TCP/IP, peut être chiffré par TLS). La politique de mot de passe fournit des mécanismes visant à garantir que les utilisateurs changent leur mot de passe périodiquement et que les mots de passe satisfont aux exigences de qualité et ne peuvent pas être réutilisés pendant une période donnée. Un utilisateur peut également se voir refuser l'accès après un certain nombre d'échecs d'authentification;

c) nom et mot de passe protégé (autrement dit un mot de passe qui est haché avec d'autres informations afin de pouvoir détecter toute tentative d'accès à l'annuaire en réutilisant la même valeur de hachage); et

d) authentification forte, pour laquelle l'expéditeur signe numériquement certaines informations. Les informations signées comprennent le nom du destinataire et d'autres informations qui permettent de détecter toute tentative de réutilisation.

Le niveau requis de protection des données est différent suivant le type d'utilisateur qui cherche à accéder aux données. Le niveau d'authentification d'un utilisateur a également une incidence sur les droits d'accès de cet utilisateur.

6.1.3 Contrôle d'accès à l'annuaire

Le contrôle d'accès est utilisé pour permettre ou refuser des opérations sur certaines informations de l'annuaire. La Recommandation UIT-T X.500 est très souple quant à la question de savoir comment subdiviser les informations d'annuaire et les utilisateurs aux fins du contrôle d'accès. Une information protégée est appelée élément protégé. Les éléments protégés pour lesquels les propriétés de contrôle d'accès sont communes peuvent être regroupés. De même, les utilisateurs peuvent être regroupés en fonction des permissions ou des refus d'accès.

Les droits d'accès d'un utilisateur ou d'un groupe d'utilisateurs dépendent du niveau d'authentification. Le niveau d'authentification requis pour consulter des informations sensibles ou pour mettre à jour des entrées sera en principe plus élevé que celui qui est requis pour consulter des informations moins sensibles.

Le contrôle d'accès tient compte également du type d'accès aux données, par exemple lecture, adjonction, suppression, mise à jour et changement de noms. Dans certains cas, il se peut que les utilisateurs ne soient même pas au courant de l'existence de certaines informations.

Le contrôle d'accès se rapporte au droit de savoir, mais dépend du besoin de savoir. Avoir le *droit de savoir* ne permet pas à un utilisateur de consulter des informations si le *besoin de savoir* n'est pas établi. Si le *besoin de savoir* n'est pas établi, la divulgation d'informations pourrait constituer une violation du respect de la vie privée.

Il existe plusieurs exemples dans lesquels le *droit de savoir* ne suffit pas, par exemple:

– même si un utilisateur a le droit de consulter les adresses postales individuelles de certaines entités, il peut être inopportun de permettre la consultation d'un grand nombre d'adresses postales;

– si un utilisateur possède des droits d'accès à certaines informations, ces droits ne s'appliquent peut-être pas à l'application particulière pour laquelle la consultation est réalisée, auquel cas il n'existe pas de *besoin de savoir* et les informations ne devraient pas être communiquées.

6.1.4 Protection de la confidentialité

La protection de la confidentialité des données décrite dans la Recommandation UIT-T X.500 est unique et très puissante. La confidentialité des données peut être mise en danger lorsqu'un utilisateur fait une recherche dans l'annuaire en fournissant des critères de recherche généraux qui pourraient donner un très grand nombre de résultats. (On parle parfois de *pêche aux informations*.)

La Recommandation UIT-T X.500 utilise un concept d'administration de service reposant sur des tables qui, en plus de l'administration des services généraux, permet aussi d'assurer une protection de la confidentialité des données. L'administrateur crée une ou plusieurs tables pour chaque combinaison de type de service et de groupe d'utilisateurs. Pour que la consultation de données aboutisse, il faut avoir une table qui corresponde exactement au type de service et au type de groupe d'utilisateurs. Toutefois, cela ne suffit pas. La table est protégée par le contrôle d'accès, autrement dit l'utilisateur doit aussi avoir la permission d'accéder à la table en question.

Une table, également appelée règle de recherche, peut contenir des informations telles que:

- les critères de recherche requis, afin de cibler la recherche pour qu'elle donne un seul ou très peu de résultats, ce qui permet d'éviter que des recherches donnent de très nombreux résultats et d'assurer une protection contre la pêche aux données;

- une liste d'informations se rapportant au type de service; et

- des informations de contrôle des différentes entités représentées dans l'annuaire. La table utilisée interagit avec les informations de contrôle d'une entité afin de restreindre les informations renvoyées concernant cette entité. Cela permet d'adapter les données en fonction des critères de protection de la confidentialité pour chaque entité particulière. Les entités peuvent avoir des exigences spéciales, elles peuvent par exemple exiger que leur adresse postale ne soit pas divulguée et éventuellement qu'une fausse adresse soit renvoyée à la place ou encore que leur adresse de courrier électronique ne soit pas communiquée à certains groupes d'utilisateurs.

La protection des informations personnelles sensibles est importante pour plusieurs raisons. Plusieurs normes sur la sécurité, notamment celles qui ont trait à l'authentification des individus et à la gestion d'identité, reposent sur la collecte et le stockage d'informations d'identification personnelle sensibles. Dans un nombre croissant de juridictions, il existe des dispositions légales relatives à la collecte et à l'utilisation de ces informations. Les services et mécanismes de sécurité, qui sont nombreux à être fondés sur des normes de l'UIT-T, servent à protéger les informations qui sont sensibles du point de vue du respect de la vie privée. Le respect de la vie privée est abordé dans un certain nombre de Recommandations, dont certaines examinent directement l'impact de certaines technologies sur le respect de la vie privée. On peut citer par exemple la Recommandation UIT-T X.1171, qui est examinée plus en détail dans le paragraphe 10.5 (Services par étiquette), et les lignes directrices sur la protection des informations d'identification personnelle dans les applications RFID, qui sont en cours d'élaboration par la Commission d'études 17 dans le cadre des travaux sur la gestion d'identité (voir paragraphe 6.4).

6.2 Authentification forte: mécanismes de sécurité à clé publique

Une infrastructure de clé publique (PKI, *public key infrastructure*) facilite la gestion des clés publiques pour assurer les services d'authentification, de chiffrement, d'intégrité et de non-répudiation. La technologie fondamentale de l'infrastructure PKI est la cryptographie à clé publique, qui est décrite ci-après. La Recommandation UIT-T X.509 est une norme PKI d'authentification forte fondée sur des certificats de clé publique et des autorités de certification. En plus de la définition d'un cadre d'authentification pour l'infrastructure PKI, la Recommandation UIT-T X.509 définit aussi une infrastructure de gestion de privilège (PMI, *privilege management infrastructure*), qui sert à vérifier les droits et privilèges des utilisateurs dans le contexte d'une autorisation forte, fondée sur des certificats d'attribut et des autorités d'attribut. Les composants des infrastructures PKI et PMI sont illustrés sur la Figure 9.

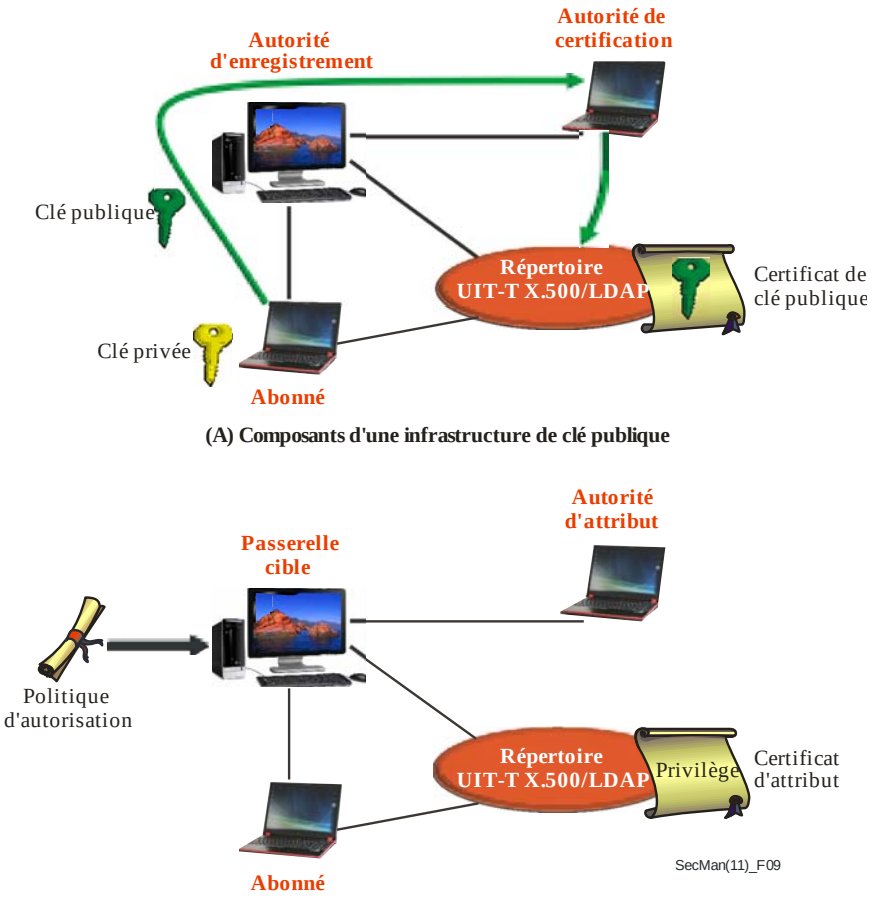


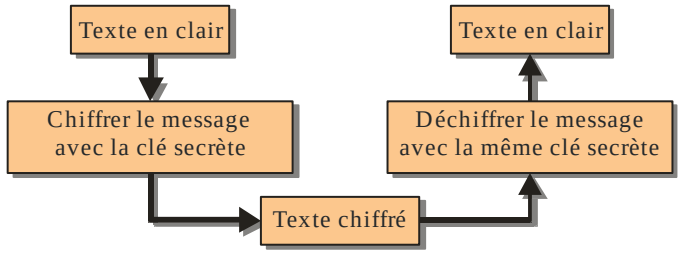
Figure 9 – Composants des infrastructures PKI et PMI

6.2.1 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 10 (a). Les individus en communication partagent donc une clé secrète unique. La clé doit être distribuée aux individus par des moyens sécurisés, car la possession de la clé de chiffrement implique la possession de la clé de déchiffrement et inversement.

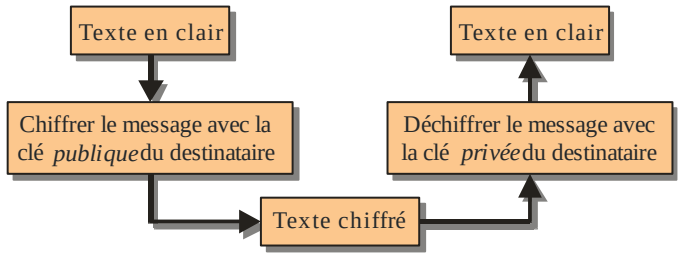
Un système de cryptographie *asymétrique* (ou à *clé publique*) fait intervenir deux clés, une clé publique et une clé privée, comme illustré sur la Figure 10 (b). La clé publique peut être distribuée largement alors que la clé privée doit toujours être gardée secrète. La clé privée est généralement conservée sur une carte à puce ou sur un jeton. La clé publique est produite à partir de la clé privée et, bien que ces clés soient liées

mathématiquement, il est impossible d'inverser le processus afin de déduire la clé privée de la clé publique. Pour envoyer à un destinataire des données confidentielles en toute sécurité en utilisant le chiffrement à clé publique, l'expéditeur chiffre les données avec la clé publique du destinataire et le destinataire les déchiffre avec sa clé privée correspondante. On peut aussi utiliser le chiffrement à clé publique pour appliquer une signature numérique à des données, le but étant de fournir la confirmation qu'un document ou un message provient bien de la personne qui déclare être l'expéditeur (ou l'auteur). La signature numérique est en réalité un condensé des données qui est produit au moyen de la clé privée du signataire et ajouté au document ou au message. Le destinataire utilise la clé publique du signataire pour confirmer la validité de la signature numérique. (Note – Certains systèmes à clé publique utilisent deux paires distinctes de clés publique/privée, l'une pour le chiffrement/déchiffrement, l'autre pour l'établissement/vérification de la signature numérique.)



– Les deux parties partagent une même clé secrète
– Problème: il est difficile d'échanger des clés dans un secret complet et ce type de chiffrement est difficilement applicable à une large communauté d'utilisateur
– Exemple le plus connu: DES (norme de chiffrement de données)

(a) Chiffrement à clé secrète (symétrique)



– Chaque participant a:
  - une clé privée qu'il ne partage avec personne d'autre
  - une clé publique que tout le monde connaît
– Problème: plus lent que le chiffrement à clé secrète
– Exemple le plus connu: RSA

(b) Chiffrement à clé publique (asymétrique)

SecMan(11)_F10

Figure 10 – Illustration des processus de chiffrement à clé secrète et à clé publique

Avec le chiffrement symétrique, chaque paire d'utilisateurs doit avoir des clés différentes et ces clés doivent être distribuées et conservées en toute sécurité. En revanche, avec le chiffrement asymétrique, les clés de chiffrement publiques peuvent être publiées dans l'annuaire et chacun peut utiliser la même clé de chiffrement (publique) pour envoyer des données à un utilisateur donné de façon sécurisée. Ainsi, le chiffrement asymétrique est beaucoup plus facilement applicable à une large communauté que le chiffrement symétrique. Toutefois, le chiffrement asymétrique nécessite de très longs calculs, de sorte qu'il est inefficace de chiffrer des messages entiers au moyen du chiffrement asymétrique. Dans la pratique, le chiffrement asymétrique est généralement utilisé pour distribuer des clés de chiffrement symétriques de façon sécurisée. Les clés symétriques sont ensuite utilisées pour chiffrer le corps du message au moyen d'un algorithme symétrique plus efficace sur le plan des calculs. Lorsqu'une signature numérique est requise, un condensé (ou une valeur de hachage) du message est produit au moyen d'une fonction de hachage unidirectionnelle

sécurisée telle que SHA-1 ou MD5. La valeur de hachage est ensuite chiffrée (au moyen de la clé privée de l'expéditeur) puis jointe au message. Le destinataire peut confirmer la validité de la signature numérique en déchiffrant la signature numérique au moyen de la clé publique de l'expéditeur pour obtenir la valeur de hachage générée par l'expéditeur puis en créant sa propre valeur de hachage du message reçu. Les deux valeurs de hachage doivent être identiques pour que la signature soit valable.

Quel que soit le mode de chiffrement (symétrique ou asymétrique) utilisé, il est impossible d'acheminer des messages entièrement chiffrés (y compris les en-têtes) à leurs destinataires, car les nœuds intermédiaires ne pourraient pas déterminer l'adresse du destinataire. Par conséquent, les en-têtes de message ne doivent généralement pas être chiffrés.

La sécurité de fonctionnement d'un système à clé publique dépend fortement de la validité des clés publiques. Les clés publiques sont normalement publiées sous la forme de certificats numériques qui sont conservés dans un annuaire UIT-T X.500. Un certificat contient non seulement la clé de chiffrement publique et, le cas échéant, la clé de vérification de la signature pour un individu, mais aussi d'autres informations, dont la validité du certificat. En principe, les certificats qui ont été révoqués pour une raison ou pour une autre sont aussi inscrits sur une liste de révocation de certificats (CRL, *certificate revocation list*) figurant dans l'annuaire. Avant d'utiliser des clés publiques, on vérifie normalement la liste CRL pour s'assurer de leur validité.

6.2.2 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 à son propriétaire et il est signé numériquement par une 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 Recommandation UIT-T X.509. Un certificat de clé publique UIT-T 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 période de validité du certificat, le numéro de la version UIT-T 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 signé numériquement au moyen de la clé privée de l'autorité de certification. Un certificat UIT-T X.509 peut être publié largement, par exemple sur un site web, dans un annuaire ou sur une carte de visite électronique (Vcard[1]) jointe à des courriers électroniques. La signature de l'autorité de certification garantit que le contenu du certificat ne peut pas être modifié sans que cela ne soit détecté.

Pour confirmer la validité d'un certificat, l'utilisateur a besoin de pouvoir accéder à la clé publique valable de l'autorité de certification qui a délivré ce certificat, afin de vérifier la signature de l'autorité de certification sur ce certificat. Etant donné que la clé publique d'une autorité de certification peut être certifiée par une autre autorité de certification (supérieure), la validation des clés publiques peut alors faire intervenir une chaîne de certificats et d'autorités de certification. Au bout du compte, cette chaîne doit avoir une fin, qui correspond généralement au certificat de l'autorité de certification qui constitue la "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 permet alors à un utilisateur de confirmer que la clé et le nom de l'autorité de certification n'ont pas été altérés depuis la création du certificat. Toutefois, le nom de l'autorité de certification figurant dans un

[1] Une vCard est une carte de visite électronique de format standard qui est souvent échangée par courrier électronique.

certificat autosigné ne peut pas être automatiquement considéré comme étant correct, 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 soient distribuées de manière sécurisée, afin de garantir qu'une clé publique appartient réellement à l'autorité de certification racine dont le nom figure dans le certificat autosigné. Sans cette garantie, l'utilisateur ne peut pas être sûr que l'identité de l'autorité de certification racine n'est pas usurpée.

6.2.3 Infrastructures de clé publique

L'infrastructure de clé publique est principalement destinée à délivrer et gérer les certificats de clé publique, y compris les certificats 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. La Recommandation UIT-T X.509 définit des mécanismes permettant de distribuer certaines de ces informations de politique dans les champs d'extension des certificats UIT-T X.509 délivrés 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 commune permettant d'évaluer la confiance que l'on peut avoir concernant les certificats délivrés par les autorités de certification, à la fois sur le plan international et d'un secteur à l'autre. Ils constituent aussi une partie du cadre juridique nécessaire à l'établissement d'une confiance interorganisations et à la spécification de restrictions quant à l'utilisation des certificats délivrés.

Les premières versions de la Recommandation UIT-T X.509 (1988, 1993 et 1997) spécifiaient les éléments de base nécessaires pour les infrastructures de clé publique et définissaient notamment les certificats de clé publique. La Recommandation UIT-T X.509 révisée qui a été approuvée en 2001 (et mise à jour en 2005 et 2008) contient des précisions sur les certificats d'attribut et définit un cadre pour l'infrastructure de gestion de privilège (PMI, *privilege management infrastructure*).

6.2.4 Infrastructure de gestion de privilège

Une infrastructure de gestion de privilège (PMI) gère les privilèges pour prendre en charge un service d'autorisation complet en relation avec une infrastructure PKI. Les mécanismes définis permettent d'établir des privilèges d'accès pour les utilisateurs dans un environnement multifabricant et multi-application. Les infrastructures PMI et PKI utilisent des concepts analogues, mais l'infrastructure PMI concerne l'autorisation tandis que l'infrastructure PKI concerne l'authentification. Le Tableau 5 illustre les analogies entre les deux infrastructures.

Tableau 5 – 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	Autorité de certification
Certificat d'attribut	Certificat de clé publique
Liste de révocation de certificats d'attribut	Liste de révocation de certificats
Liste de révocation d'autorités pour l'infrastructure PMI	Liste de révocation d'autorités 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 la politique sont rattachées au nom d'utilisateur dans le certificat d'attribut et comprennent un certain nombre d'éléments illustrés dans le Tableau 6.

Tableau 6 – Structure d'un certificat d'attribut UIT-T X.509

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

Les certificats d'attribut sont également utilisés en télébiométrie (voir le paragraphe 6.5) afin de créer des certificats biométriques pour rattacher un utilisateur à ses informations biométriques. Les certificats de dispositif biométrique définissent les capacités et les limitations des dispositifs biométriques. Les certificats de politique biométrique définissent la relation entre un niveau de sécurité et des paramètres d'algorithme biométrique.

Cinq composants sont décrits dans la Recommandation UIT-T X.509 pour le contrôle de l'infrastructure PMI: le déclarant de privilège, le vérificateur de privilège, la méthode objet, la politique de privilège et les variables d'environnement (voir la Figure 11). Le vérificateur de privilège peut contrôler l'accès du déclarant de privilège à la méthode objet, conformément à la politique de privilège.

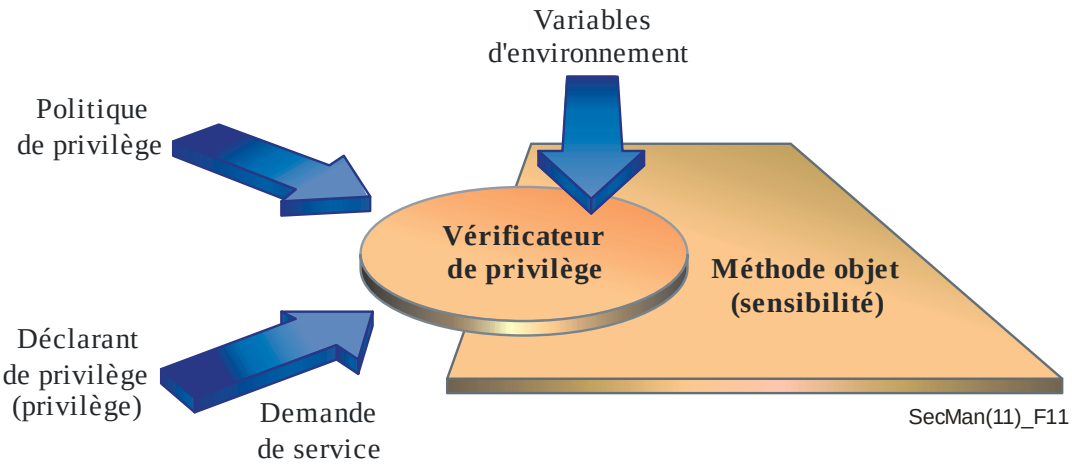


Figure 11 – Modèle de contrôle de l'infrastructure PMI UIT-T X.509

Pour certaines mises en oeuvre, il peut être nécessaire de déléguer un privilège. Quatre composants sont pris en considération dans la Recommandation UIT-T X.509 pour le modèle de délégation pour l'architecture PMI: le vérificateur de privilège, la source d'autorité, d'autres autorités d'attribut et le déclarant de privilège (voir la Figure 12).

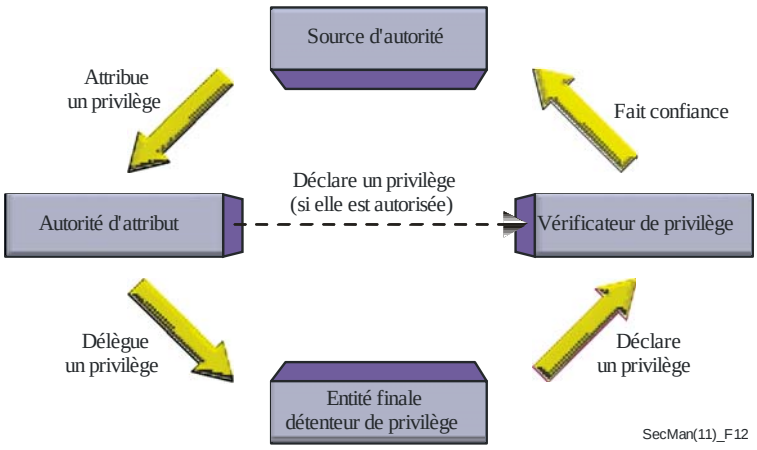


Figure 12 – Modèle de délégation pour l'infrastructure PMI UIT-T X.509

Dans les mises en oeuvre récentes de systèmes d'autorisation fondées sur le modèle du contrôle d'accès basé sur le 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.

6.3 Lignes directrices relatives à l'authentification

Un certain nombre de lignes directrices portant sur des aspects spécifiques de l'authentification ont été élaborées. Elles sont récapitulées ci-dessous.

6.3.1 Protocole d'authentification sûre fondée sur un mot de passe avec échange de clés

Le protocole d'authentification sûre fondée sur un mot de passe avec échange de clés (SPAK, *secure password-based authentication protocol with key exchange*) est un protocole d'authentification simple dans lequel l'utilisation d'un mot de passe facilement mémorisable entre un client et un serveur permet de procéder à une authentification mutuelle et d'utiliser un secret partagé comme clés de session pour la session suivante.

Les exigences relatives au protocole SPAK et les lignes directrices permettant de choisir celui qui convient le mieux parmi divers protocoles d'authentification sûre fondée sur un mot de passe sont définies dans la Recommandation UIT-T X.1151. Ce protocole est très simple. Il est facile à mettre en œuvre et à utiliser et, contrairement au protocole PKI, ne nécessite pas d'autre infrastructure. Il devrait gagner en importance pour de nombreuses applications futures. Le protocole SPAK permet à la fois une authentification de l'utilisateur et un échange de clés avec un simple mot de passe. Une session de communication à venir peut ainsi être protégée par un secret qui est partagé pendant la procédure d'authentification (voir la Figure 13).

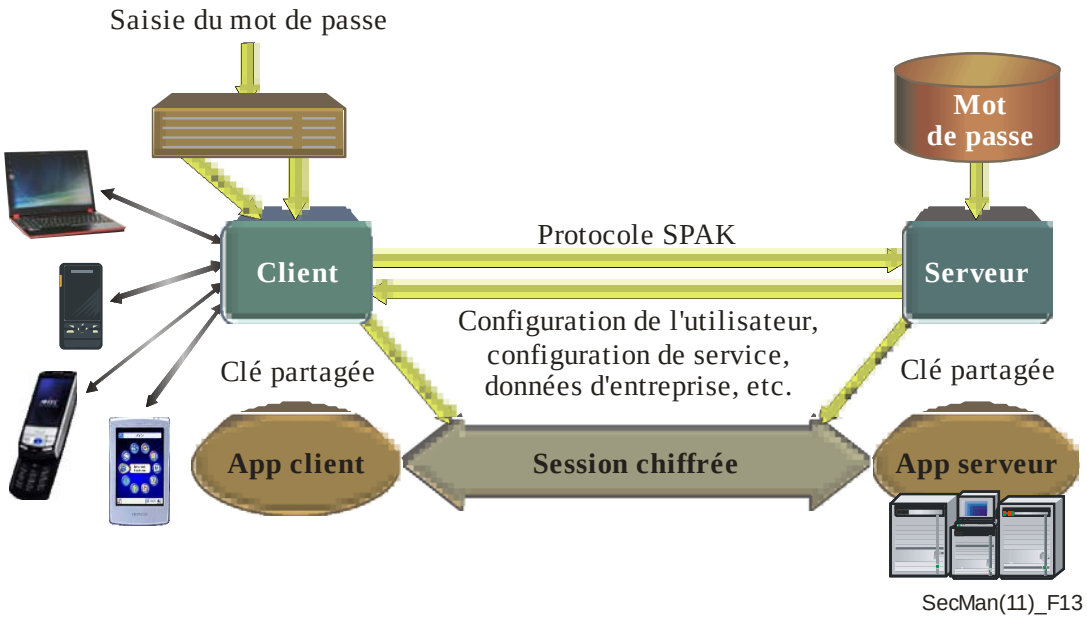


Figure 13 – Fonctionnement type du protocole SPAK

6.3.2 Protocole d'authentification extensible

Le protocole d'authentification extensible (EAP, *extensible authentication protocol*) prend en charge plusieurs mécanismes d'authentification entre un demandeur et un serveur d'authentification dans un réseau de communication de données. Le protocole EAP peut servir d'outil de base pour l'activation de l'authentification de l'utilisateur et la distribution des clés de session. Il peut permettre d'authentifier un dispositif afin d'établir une connexion point à point sécurisée et d'interdire l'accès aux dispositifs non autorisés.

La Recommandation UIT-T X.1034 décrit un cadre applicable à l'authentification et à la gestion de clé basées sur le protocole EAP pour sécuriser les couches inférieures dans un réseau de communication. Elle donne des indications sur le choix des méthodes EAP et décrit le mécanisme de gestion de clé pour les couches inférieures d'un réseau de communication de données. Le cadre s'applique à la fois aux réseaux d'accès sans fil et aux réseaux d'accès filaires avec un support partagé.

Trois entités sont nécessaires pour l'authentification et la gestion de clé: un demandeur (ou homologue), un authentificateur et un serveur d'authentification, comme indiqué sur la Figure 14. Le demandeur fonctionne comme un utilisateur final, qui accède au réseau depuis une station d'utilisateur final. L'authentificateur joue le rôle d'entité d'application de politiques, qui relaie les messages EAP entre le demandeur et le serveur d'authentification. Le serveur d'authentification authentifie le demandeur, partage facultativement un secret qui peut être utilisé pour déduire des clés de chiffrement, envoie le résultat de l'authentification à l'authentificateur, et retransmet le secret partagé à l'authentificateur. Ce secret partagé peut servir à déduire des clés de chiffrement entre l'authentificateur et le demandeur pour garantir la confidentialité et l'intégrité et permettre l'authentification des messages.

L'authentification et la gestion de clé comprennent généralement quatre phases: découverte des capacités de sécurité, authentification EAP, distribution de clé, gestion de clé (voir la Figure 14). Dans la phase relative aux capacités de sécurité, le demandeur négocie les capacités de sécurité et les divers paramètres du protocole à utiliser avec l'authentificateur. Dans la phase EAP, le serveur d'authentification authentifie le demandeur et déduit un secret principal partagé avec le demandeur. Dans la phase de distribution de clé, le serveur d'authentification transmet le secret principal à l'authentificateur pour permettre de déduire des clés de chiffrement pour une session à venir entre le demandeur et l'authentificateur. (Il convient d'utiliser de nouvelles clés de chiffrement dans chaque session.) Enfin, dans la phase de gestion de clé, l'authentificateur

échange des nombres aléatoires avec le demandeur pour obtenir une nouvelle clé de chiffrement, conduisant à une confidentialité parfaite.

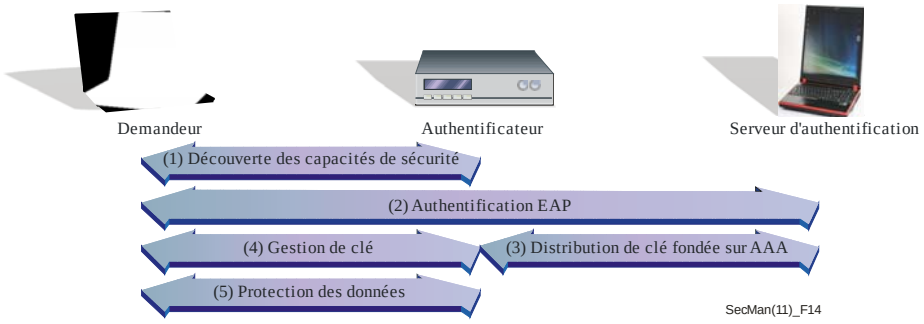


Figure 14 – Phases pour l'authentification et la gestion de clé pour la couche inférieure

6.3.3 Authentification par mot de passe à usage unique

L'emploi d'un mot de passe à usage unique (OTP) améliore la sécurité, tout en évitant le risque que le mot de passe soit deviné et réutilisé. L'authentification reposant sur un mot de passe à usage unique peut être utilisée conjointement avec d'autres mécanismes d'authentification (par exemple, une infrastructure PKI ou un mot de passe statique) pour prendre en charge l'authentification à plusieurs facteurs. La Recommandation UIT-T X.1153 définit un cadre de gestion pour l'authentification reposant sur un mot de passe à usage unique et présente un cadre de gestion interopérable qui permet le partage d'un seul jeton de mot de passe à usage unique entre différents fournisseurs de services.

6.4 Gestion d'identité

6.4.1 Aperçu de la gestion d'identité

La gestion d'identité (IdM, *identity management*) consiste à gérer de façon sécurisée et à contrôler les informations d'identité (par exemple justificatifs, identificateurs, attributs et réputations) qui sont utilisées pour représenter les entités (fournisseurs de services, organisations d'utilisateurs finals, personnes, dispositifs de réseau, applications logicielles et services) dans un processus de communications. Une même entité peut avoir plusieurs identités numériques afin d'accéder à divers services avec différentes exigences, ces identités pouvant exister à plusieurs endroits. L'IdM prend en charge l'authentification d'une entité. Aux fins de l'UIT-T, l'identité déclarée par une entité représente l'unicité de cette entité dans un contexte donné.

L'IdM est essentielle pour la cybersécurité, car elle permet d'établir et de maintenir des communications fiables entre les entités et permet un accès nomade à la demande aux réseaux et aux cyberservices. Elle permet aussi d'autoriser toute une gamme de privilèges (et non des privilèges tout ou rien) et facilite la modification des privilèges en cas de changement de rôle d'une entité. L'IdM permet à une organisation de mieux appliquer ses politiques de sécurité grâce à la possibilité de surveiller et de vérifier les activités d'une entité sur le réseau. Elle facilite en outre l'accès aux entités aussi bien à l'intérieur qu'à l'extérieur d'une organisation.

L'IdM permet de garantir des informations d'identité, avec un contrôle d'accès sécurisé, ce qui est possible grâce à la connexion unique/déconnexion unique, au contrôle par l'utilisateur des informations d'identification personnelle et à la possibilité pour un utilisateur de choisir un fournisseur d'identité qui peut assurer des fonctions de vérification et de délégation pour son compte, par opposition à la fourniture de justificatifs à chaque fournisseur de services. L'IdM prend également en charge une multitude de services fondés sur l'identité: publicité ciblée, services personnalisés basés sur l'emplacement géographique et l'intérêt, services avec authentification pour diminuer la fraude et le vol d'identité, etc.

L'IdM est une technologie complexe qui inclut:

- l'établissement, la modification, la suspension, l'archivage et la suppression d'informations d'identité;
- la reconnaissance d'identités partielles qui représentent des entités dans un contexte ou un rôle spécifique;
- l'établissement et l'évaluation de la confiance entre des entités; et
- la localisation des informations d'identité d'une entité (par exemple via un fournisseur d'identité faisant autorité qui est légalement responsable de la conservation des identificateurs, des justificatifs et de tout ou partie des attributs de l'entité).

Le Supplément 7 aux Recommandations UIT-T de la série X présente brièvement ce qu'est la gestion d'identité.

6.4.2 Travaux de l'UIT-T sur la gestion d'identité

Les travaux portant sur l'IdM sont essentiellement menés dans le cadre de deux commissions d'études, comme indiqué ci-dessous.

La Commission d'études 17, Commission d'études directrice pour l'IdM, est chargée d'étudier l'élaboration d'un modèle générique de gestion d'identité, indépendant des technologies de réseau et prenant en charge l'échange sécurisé d'informations d'identité entre des entités. Il s'agit aussi d'étudier le processus de découverte des sources d'informations d'identité qui font autorité, les mécanismes génériques pour l'interopérabilité de divers formats d'informations d'identité, les menaces liées à la gestion d'identité, les mécanismes de lutte contre ces menaces et la protection des informations d'identification personnelle (PII) et d'élaborer des mécanismes garantissant que l'accès aux informations PII n'est autorisé que lorsque cet accès est approprié. Les Recommandations relatives à la gestion d'identité approuvées à ce jour sont les suivantes: Recommandations UIT-T X.1250, UIT-T X.1251, UIT-T X.1253 et UIT-T X.1275. Par ailleurs, la Recommandation UIT-T X.1252, *Termes et définitions de base relatifs à la gestion d'identité*, fournit un ensemble de définitions liées à la gestion d'identité pour faire en sorte que les normes sur la gestion d'identité emploient une terminologie uniforme et cohérente. Les travaux sur l'établissement d'un cadre applicable aux certificats de validation étendue et d'un cadre commun ISO/UIT-T de garantie d'authentification des entités sont sur le point d'être achevés.

La Commission d'études 13 (Réseaux futurs, y compris les réseaux mobiles et les réseaux de prochaine génération (NGN)) mène des études se rapportant à une architecture fonctionnelle de gestion d'identité propre aux réseaux NGN qui prend en charge des services d'identité à valeur ajoutée, l'échange sécurisé d'informations d'identité et l'interopérabilité entre divers formats d'informations d'identité. Elle mène également des études se rapportant à la détermination des menaces liées à la gestion d'identité dans les réseaux NGN et des mécanismes de lutte contre ces menaces. La Recommandation UIT-T Y.2720 décrit une approche structurée pour concevoir, définir et mettre en œuvre des solutions IdM et faciliter l'interopérabilité dans des environnements hétérogènes. La CE 13 a élaboré deux autres Recommandations relatives à la gestion d'identité, à savoir la Recommandation UIT-T Y.2721, qui décrit des objectifs et des exigences et fournit une analyse d'exemples de cas d'utilisation, et la Recommandation ITU-T Y.2722, qui spécifie les mécanismes pouvant être utilisés pour satisfaire aux exigences de la gestion d'identité et aux besoins de déploiement des réseaux de prochaine génération.

Une activité conjointe de coordination pour la gestion d'identité (JCA-IdM) est en place depuis 2007. La mission de la JCA-IdM est de coordonner les activités relatives à la gestion d'identité menées au sein de l'UIT-T et avec d'autres organisations. Cette JCA a créé une page web de sources d'informations relatives à la gestion d'identité, qui recense les documents relatifs à la gestion d'identité émanant de l'UIT-T et d'autres

organisations de normalisation, et les classe par catégorie, organisation et état d'avancement des travaux. La page web de la Commission d'études directrice pour la gestion d'identité contient de nombreuses informations sur les activités dans ce domaine, les Recommandations approuvées et les Recommandations en cours d'élaboration sur la gestion d'identité et d'autres informations sur les travaux relatifs à la gestion d'identité. On trouvera ce "panorama" de la gestion d'identité à l'adresse: http://groups.itu.int/itu-t/StudyGroups/SG17/IdmRoadmap.aspx.

6.5 Télébiométrie

La télébiométrie vise à identifier et à authentifier les personnes au moyen de dispositifs biométriques dans des environnements de télécommunication. L'un des objectifs est d'améliorer la sûreté et la sécurité de l'identification ou de l'authentification des utilisateurs grâce à l'utilisation de méthodes télébiométriques. Les travaux de l'UIT-T dans ce domaine sont menés en étroite coopération avec d'autres organisations de normalisation et leurs résultats à ce jour portent sur: l'interaction entre un être humain et l'environnement, les clés numériques biométriques, les extensions biométriques des certificats UIT-T X.509 et l'authentification biométrique dans un réseau ouvert.

6.5.1 Authentification télébiométrique

La biométrie permet d'offrir des services d'authentification hautement sécurisés, mais la normalisation de l'authentification biométrique sur un réseau ouvert fait face à un certain nombre de problèmes:

- il se peut que les fournisseurs de services ne soient pas informés des dispositifs biométriques qui sont utilisés dans l'environnement de l'utilisateur final, du niveau ou des paramètres de sécurité de ces dispositifs, ou de leur mode de fonctionnement;

- la précision (telle qu'elle est déterminée par le taux de fausses acceptations ou de rejets erronés) varie en fonction des produits biométriques. Le fournisseur de services ne peut donc pas déclarer maintenir un niveau de précision uniforme; et

- la précision de la vérification biométrique dépend à la fois de facteurs environnementaux (par exemple, l'éclairage ou la météo) et de facteurs humains (par exemple, la pose, le maquillage ou les caractéristiques des verres de contact et le vieillissement).

Les protocoles généraux d'authentification biométrique et les profils pour les systèmes de télécommunication dans un réseau ouvert sont spécifiés dans la Recommandation UIT-T X.1084.

La Figure 15 illustre l'authentification d'un utilisateur final via un réseau ouvert sans contact direct.

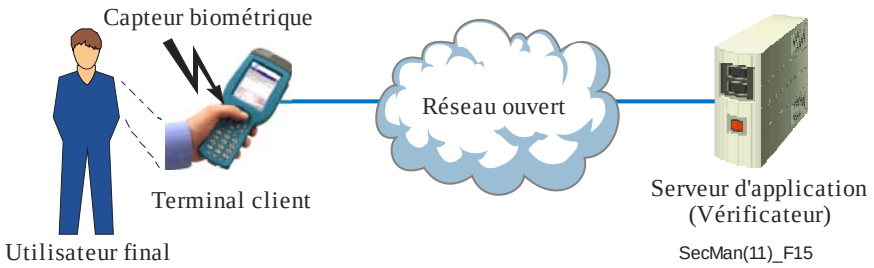


Figure 15 – Authentification télébiométrique d'un utilisateur final

6.5.2 Génération et protection des clés numériques télébiométriques

Un cadre pour la génération et la protection des clés numériques biométriques a été défini dans la Recommandation UIT-T X.1088. Ce cadre définit la protection sur la base d'un modèle biométrique avec un certificat de clé publique et un certificat biométrique afin d'assurer une authentification sécurisée par le chiffrement et des communications sécurisées sur des réseaux ouverts. Des exigences de sécurité sont également définies pour la génération et la protection des clés numériques biométriques. Le cadre peut être appliqué au chiffrement biométrique et à la signature numérique. Deux méthodes sont proposées:

- génération de clé biométrique, dans laquelle la clé est créée à partir d'un modèle biométrique (Figure 16); et

- liaison/rétablissement de clé biométrique, dans laquelle la clé est stockée dans une base de données et peut être extraite par authentification biométrique (Figure 17).

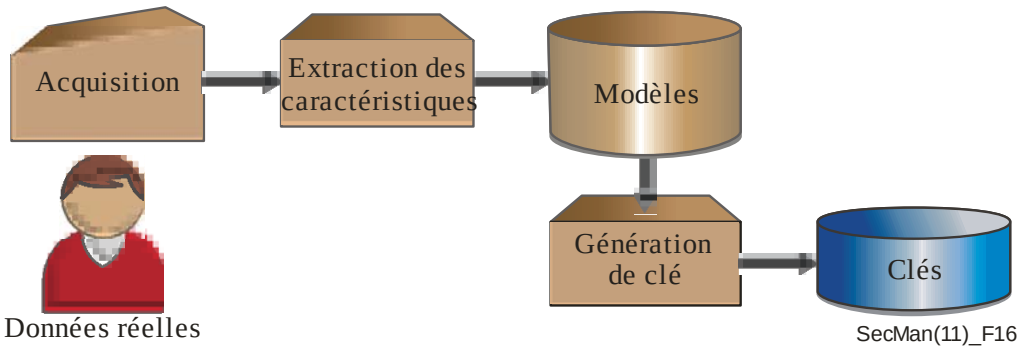


Figure 16 – Génération de clé biométrique

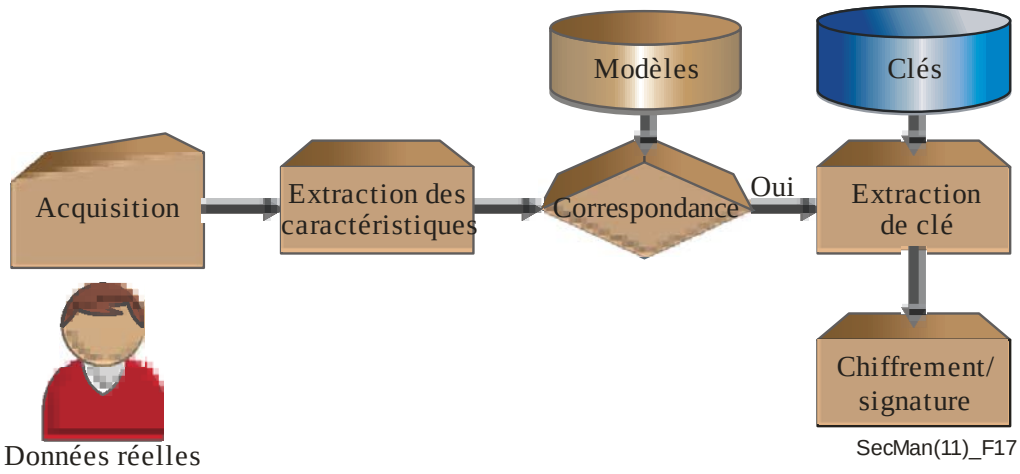


Figure 17 – Liaison/rétablissement de clé biométrique

6.5.3 Aspects de sécurité et de sûreté de la télébiométrie

Un cadre pour les aspects de sécurité et de sûreté de la télébiométrie a été défini dans le modèle multimodal télébiométrique (Recommandation UIT-T X.1081), qui définit les interactions entre un être humain et l'environnement ainsi que les grandeurs et unités utilisées pour mesurer ces interactions. Ce modèle ne se limite pas à la prise en compte des interactions purement physiques, mais il prend également en compte les interactions comportementales qui ne sont actuellement pas quantifiées par des unités standards.

La Recommandation UIT-T X.1086 ne définit pas seulement les vulnérabilités et les menaces associées aux systèmes de télébiométrie en fonctionnement, mais décrit également des contre-mesures propres à assurer la protection des dispositifs biométriques au moment de l'installation, du démontage et de la livraison. Parmi les contre-mesures spécifiées figurent les systèmes techniques de protection des procédures opérationnelles des systèmes biométriques, ainsi qu'une description des rôles et responsabilités du personnel autorisé participant à la supervision du système.

6.5.4 Télébiométrie relative à la physiologie humaine

Les aspects de sécurité et de sûreté de la télébiométrie sont également pris en compte dans la Recommandation UIT-T X.1082, qui définit des grandeurs et des unités pour les caractéristiques physiologiques, biologiques ou comportementales qui pourraient servir de données d'entrée ou de données de sortie pour des systèmes d'identification ou de vérification biométriques (systèmes de reconnaissance), y compris les seuils de détection ou de sécurité connus. Cette Recommandation donne des noms, des définitions et des symboles de grandeurs et d'unités pour la télébiométrie relative à la physiologie humaine (c'est-à-dire les caractéristiques humaines et les émissions qui peuvent être détectées par un capteur). Elle porte aussi sur des grandeurs et des unités relatives aux effets sur l'être humain causés par l'utilisation de dispositifs télébiométriques.

6.5.5 Gabarit télébiométrique à usage unique

La Recommandation UIT-T X.1090 spécifie un cadre d'authentification d'utilisateur utilisant des gabarits biométriques à usage unique. Ce cadre décrit des mécanismes d'authentification d'utilisateur sécurisée et de protection des gabarits biométriques transmis sur des réseaux ouverts, grâce à la génération d'un nouveau gabarit à usage unique pour chaque instance d'authentification.

6.5.6 Autres éléments définis dans les normes sur la télébiométrie

Des extensions ont été définies pour les certificats UIT-T X.509 utilisés dans les infrastructures de clé publique ou dans les infrastructures de gestion de privilège afin de produire des certificats biométriques. Elles sont spécifiées dans la Recommandation UIT-T X.1089. La Recommandation UIT-T X.1083 spécifie la syntaxe (utilisant l'ASN.1), la sémantique et le codage des messages qui permettent à une application conforme BioAPI de demander des opérations biométriques dans des fournisseurs de service biométrique conformes BioAPI (BSP) de part et d'autre des frontières entre des nœuds ou des processus, et de recevoir la notification des événements provenant de ces BSP distants.

Un autre aspect important de ces travaux a trait aux protocoles génériques concernant la sûreté, la sécurité, la protection de la vie privée et l'accord pour la manipulation de données biométriques dans n'importe quelle application de télébiométrie, par exemple la cybersanté, la télémédecine et la télésanté. La Recommandation UIT-T 1080.1 définit un protocole générique de télécommunication qui prend en charge les interactions entre un patient se trouvant dans un poste de secours local et un centre médical distant susceptible d'offrir de meilleures compétences.

7. Sécurisation de l'infrastructure des réseaux

7 Sécurisation de l'infrastructure des réseaux

Les données utilisées pour surveiller et contrôler le réseau de télécommunication sont souvent transmises dans un réseau distinct qui achemine uniquement le trafic de gestion de réseau (pas le trafic des utilisateurs). Ce réseau, souvent appelé réseau de gestion des télécommunications (RGT), est décrit dans la Recommandation UIT-T M.3010. Il est impératif que ce trafic soit sécurisé. Le trafic de gestion est généralement classé dans différentes catégories en fonction des informations requises pour exécuter les fonctions de gestion des dérangements, de la configuration, de la qualité de fonctionnement, de la comptabilité et de la sécurité. La gestion de la sécurité de réseau 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 de l'architecture de sécurité UIT-T X.805.

L'activité de gestion des éléments d'infrastructure d'un réseau doit toujours être entreprise de manière sécurisée. Par exemple, les activités de réseau ne doivent être réalisées que par un utilisateur autorisé. Pour pouvoir offrir une solution sécurisée de bout en bout, des mesures de sécurité (par exemple contrôle d'accès, authentification) doivent être appliquées à chaque type d'activité de réseau concernant l'infrastructure du réseau, les services de réseau et les applications de réseau. Un certain nombre de Recommandations UIT-T portent tout particulièrement sur l'aspect de sécurité du plan de gestion en ce qui concerne les éléments de réseau et les systèmes de gestion qui font partie de l'infrastructure du réseau.

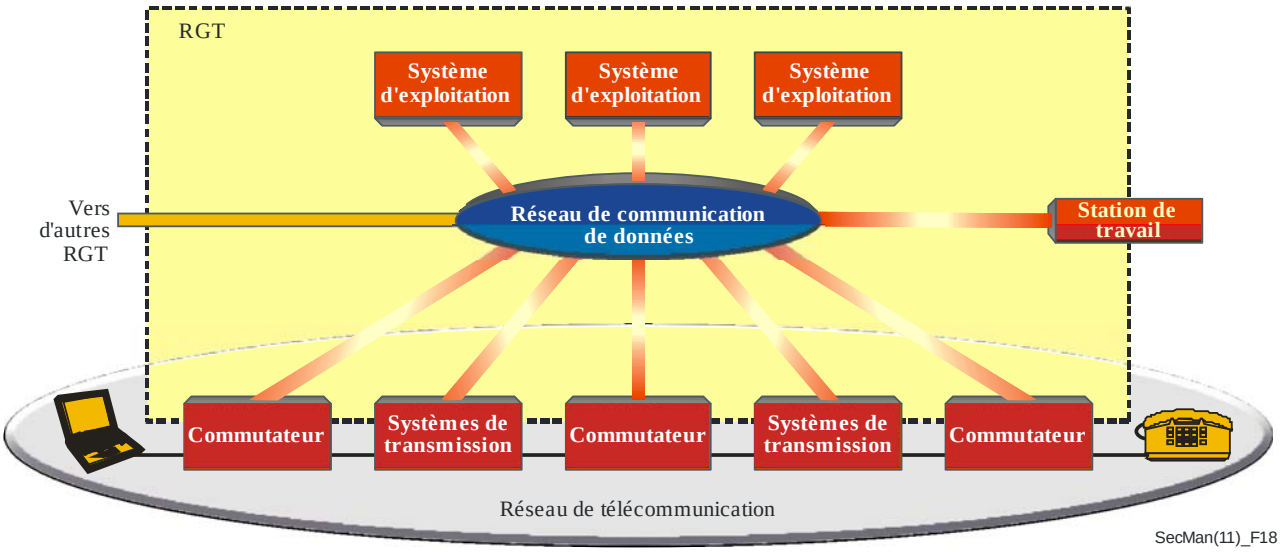
Parmi les autres applications de gestion de réseau, on peut citer celles qui se rapportent aux environnements dans lesquels différents fournisseurs de services doivent interagir pour offrir des services de bout en bout, par exemple dans le cas où des moyens de communication sont fournis à des organismes de réglementation ou à des organismes publics en vue d'assurer le retour à la normale après une catastrophe ou le cas où des lignes louées par des clients traversent des frontières géographiques.

7.1 Le réseau de gestion des télécommunications (RGT)

Le RGT est séparé et isolé de l'infrastructure du réseau public de sorte que les éventuelles 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 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, car le plan de gestion devient maintenant accessible à une multitude d'utilisateurs finals, ce qui rend possibles de nombreux autres types d'activités malveillantes qu'il faut combattre.

7.2 Architecture de gestion de réseau

L'architecture permettant de définir la gestion d'un réseau de télécommunication est définie dans la Recommandation UIT-T M.3010. La relation entre un RGT et un réseau de télécommunication est illustrée sur la Figure 18. L'architecture du réseau de gestion définit des interfaces qui déterminent les échanges requis pour assurer les fonctions d'exploitation, d'administration, de maintenance et de configuration.



NOTE – Le RGT, dont la limite est représentée en pointillés, peut aussi englober et gérer les services et équipements de clients/d'utilisateurs.

Figure 18 – Relation entre un RGT et un réseau de télécommunication

La Recommandation UIT-T M.3016.0 fournit un aperçu général et un cadre qui identifient les menaces de sécurité concernant un RGT. Dans la série UIT-T M.3016, la Recommandation UIT-T UIT-T M.3016.1 donne des détails sur les exigences de sécurité, la Recommandation UIT-T M.3016.2 décrit les services de sécurité et la Recommandation UIT-T M.3016.3 définit des mécanismes permettant de faire face aux menaces dans le contexte de l'architecture fonctionnelle du RGT définie dans la Recommandation UIT-T M.3010. Comme les exigences n'ont pas besoin d'être toutes prises en charge par toutes les organisations, la Recommandation UIT-T M.3016.4 contient un formulaire permettant de créer des profils en fonction des exigences, des services et des mécanismes de sécurité individuels, ce qui permet d'élaborer des profils conformes à la politique de sécurité propre à une organisation.

Lorsqu'on examine la gestion de la sécurité de réseau, deux aspects sont à prendre en considération. Le premier concerne le plan de gestion pour une activité de bout en bout entre utilisateurs (par exemple, les services de téléphonie IP), pour laquelle l'administration des utilisateurs doit être réalisée de manière sécurisée. On parle de *sécurité des informations de gestion* échangées sur le réseau pour la prise en charge d'une application de bout en bout. Le deuxième aspect est *la gestion des informations de sécurité*, qui s'applique quelle que soit l'application. Par exemple, l'activité de signalisation de dérangement entre deux fournisseurs de services doit être réalisée en toute sécurité. Pour cela, un chiffrement des échanges peut être nécessaire, auquel cas il faut prévoir de gérer les clés de chiffrement.

Plusieurs Recommandations portant sur des fonctions de gestion de la sécurité de l'architecture UIT-T X.805 sont disponibles pour les trois couches du plan de gestion (voir la Figure 1). De plus, comme on le verra dans les paragraphes qui suivent, d'autres Recommandations définissent des services génériques ou communs, par exemple l'envoi d'alarme en cas de violation de la sécurité, des fonctions d'audit et des modèles d'information qui définissent des niveaux de protection pour différentes cibles.

7.3 Sécurisation des éléments d'infrastructure d'un réseau

La connectivité de bout en bout peut être prise en considération 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*). L'administration des privilèges des utilisateurs pour un tel réseau d'accès est définie au moyen de la méthodologie de modélisation unifiée définie dans la Recommandation UIT-T Q.834.3. L'échange de gestion reposant sur l'architecture de courtier

commun de requêtes d'objets (CORBA, *common object request broker architecture*) est spécifié dans la Recommandation UIT-T Q.834.4. L'interface décrite dans ces Recommandations 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 19 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 la liste des activités de gestion qui sont permises pour chaque utilisateur autorisé. Le gestionnaire de contrôle d'accès vérifie l'identifiant et le mot de passe de l'utilisateur de l'activité de gestion et autorise l'accès en fonction de la fonctionnalité figurant dans la liste de permissions.

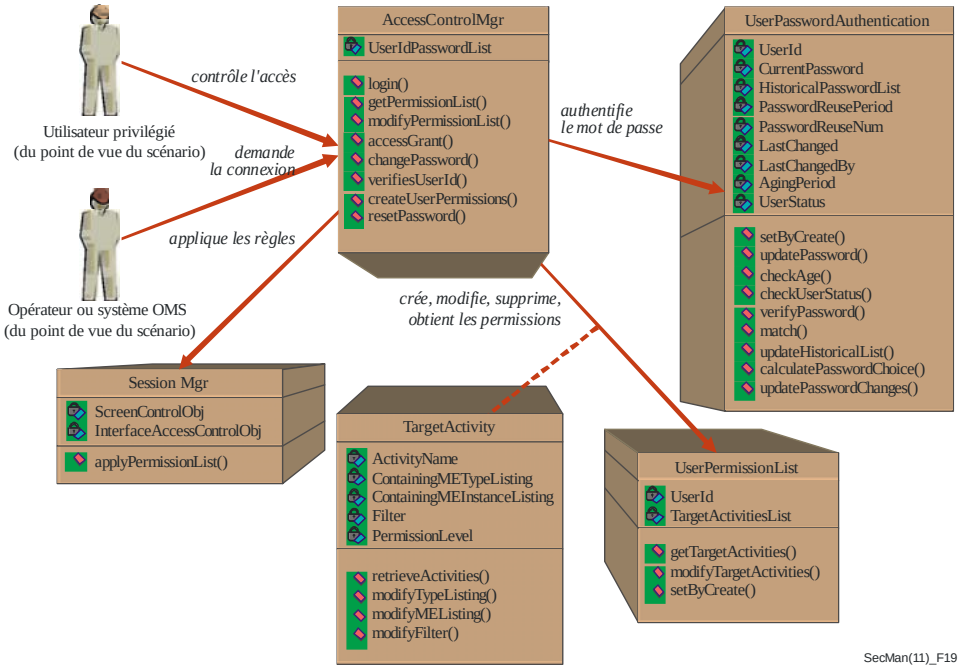


Figure 19 – Administration des privilèges des utilisateurs (UIT-T Q.834.3)

7.4 Sécurisation des activités de surveillance et de contrôle

Deux aspects de sécurité s'appliquent à l'intersection entre le plan de gestion et la couche services. Le premier aspect consiste à veiller à ce que des mesures de sécurité appropriées soient disponibles pour les services offerts dans le réseau (par exemple veiller à ce que seuls des utilisateurs valables soient autorisés à exécuter les opérations associées à la configuration d'un service). Le second aspect consiste à définir les échanges administratifs et de gestion qui sont valables afin de faciliter la détection des violations de sécurité.

La Recommandation UIT-T M.3208.2 porte sur le premier aspect, l'activité de gestion d'un service. 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 configure la connectivité de bout en bout, il est nécessaire de garantir que seuls les utilisateurs autorisés peuvent exécuter ces opérations. Les dimensions de sécurité UIT-T X.805 associées à ce service sont: l'authentification d'entité homologue, le contrôle d'intégrité des données (afin d'empêcher toute modification non autorisée des données en transit) et le 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, qui définit les activités administratives associées au plan de gestion pour les services hertziens, est un exemple de norme qui porte sur le second aspect. Dans un réseau hertzien, lorsque les utilisateurs se déplacent entre leur réseau de rattachement et un réseau visité, ils peuvent traverser différents domaines administratifs. Dans la description des services qui figure dans la Recommandation UIT-T M.3210.1, il est précisé comment le domaine de gestion des fraudes du réseau de rattachement collecte les informations appropriées concernant un abonné qui est enregistré dans un réseau visité. Les scénarios a) et b) de la Figure 20 illustrent le déclenchement de l'activité de gestion de surveillance respectivement par le réseau de rattachement et par le réseau visité. Le système de détection des fraudes du réseau de rattachement demande des informations sur les activités d'un abonné qui s'enregistre dans un réseau visité et reste actif jusqu'à ce que cet abonné annule son enregistrement dans ce réseau. Des profils d'utilisation peuvent alors être élaborés sur la base d'une analyse des relevés d'appel au niveau du service ou pour un abonné. Le système de détection des fraudes peut procéder à une analyse et produire des alarmes appropriées lorsqu'un comportement frauduleux est détecté.

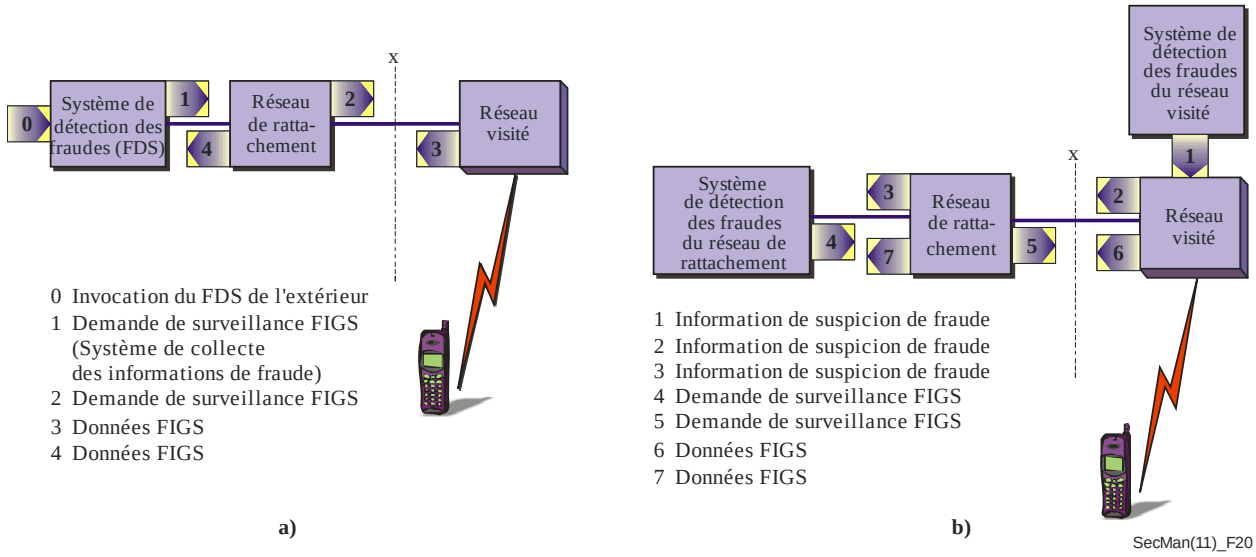


Figure 20 – Gestion des fraudes pour les services hertziens

7.5 Sécurisation des activités d'exploitation de réseau et des applications de gestion

L'intersection du plan de gestion et de la couche application dans la Recommandation UIT-T X.805 correspond à la sécurisation des applications d'utilisateur final fondées sur le réseau, par exemple la messagerie et l'annuaire. Une autre catégorie d'applications pour lesquelles les activités de gestion doivent être sécurisées est celle des applications de gestion proprement dites. La meilleure explication sera fournie au moyen d'exemples. Pour ces applications, le personnel de gestion (d'exploitation) du fournisseur de services représente les utilisateurs finals. Prenons le cas où un fournisseur de services 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 appelée *administration des dossiers de dérangement* afin de signaler le problème. L'utilisateur de ces systèmes, ainsi que l'application proprement dite, a besoin d'une autorisation pour pouvoir signaler des problèmes. Les systèmes et utilisateurs autorisés doivent prendre les mesures qui s'imposent pour extraire l'état du ou des problèmes signalés. La Figure 21 illustre les interactions qui doivent être réalisées de manière sécurisée. 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.

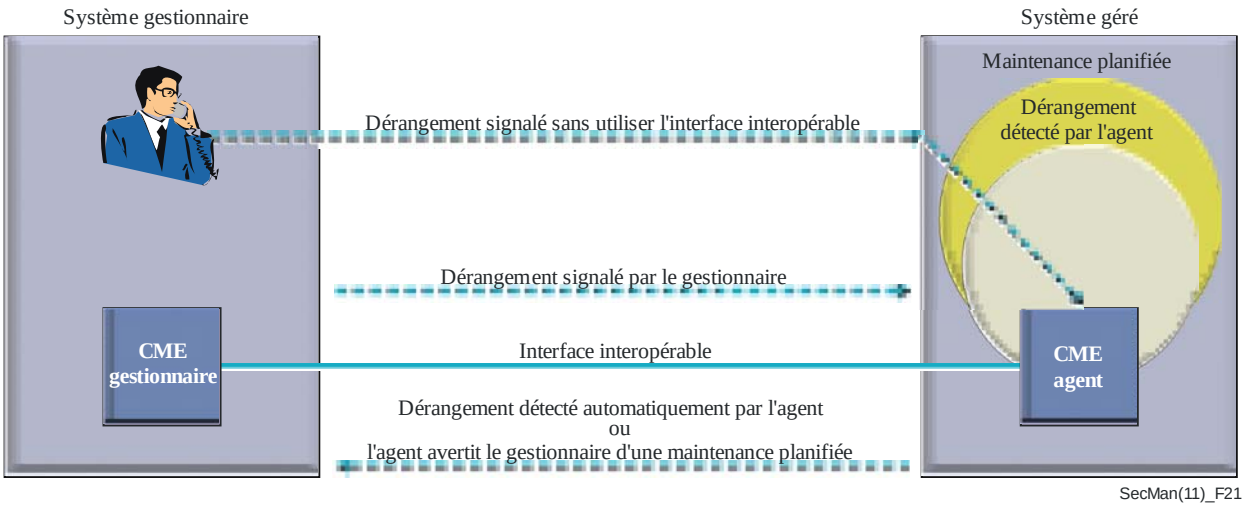


Figure 21 – Création d'un dossier de gestion de dérangement

La Recommandation UIT-T X.790 définit cette application de gestion et utilise des mécanismes tels que les listes de contrôle d'accès et l'authentification bidirectionnelle pour sécuriser les activités.

7.6 Services communs de gestion de la sécurité

Un certain nombre de services communs sont considérés comme étant des activités du plan de gestion UIT-T X.805. Ils s'appliquent en particulier lorsque le *protocole commun d'information de gestion (CMIP)* (Recommandation UIT-T X.711) est utilisé. Certains de ces services sont brièvement décrits ci-après.

7.6.1 Fonction de signalisation des alarmes de sécurité

La signalisation des alarmes est une fonction essentielle dans les interfaces de gestion. Lorsqu'une défaillance est détectée, par suite de problèmes opérationnels (par exemple défaillance de l'ensemble de circuits ou violation de la politique de sécurité), une alarme est communiquée au système de gestion. Les rapports d'alarme incluent un certain nombre de paramètres, de sorte que le système de gestion puisse déterminer le motif de la défaillance et prendre une mesure corrective. Les paramètres relatifs à un événement donné incluent un champ obligatoire appelé *type d'événement* et un ensemble d'autres champs appelés *informations d'événement*. Ces derniers champs contiennent des informations telles que la gravité de l'alarme, les motifs probables de déclenchement de l'alarme et le détecteur de la violation de sécurité. Les motifs de déclenchement des alarmes sont associés aux types d'événement comme indiqué dans le Tableau 7.

Tableau 7 – Motifs de déclenchement des alarmes de sécurité

Type d'événement	Motifs de déclenchement de l'alarme de sécurité
Violation de l'intégrité	Information dupliquée Information manquante Détection de modification d'information Information hors séquence Information inattendue
Violation opérationnelle	Refus de service Hors service Erreur de procédure Raison non spécifiée
Violation physique	Altération frauduleuse du câble Détection d'intrusion Raison non spécifiée
Violation de service ou de mécanisme de sécurité	Echec d'authentification Atteinte à la confidentialité Échec de non-répudiation Tentative d'accès non autorisée Raison non spécifiée
Violation du domaine temporel	Information tardive Mot de passe périmé Activité en dehors de l'horaire

On trouvera davantage d'explications sur ces motifs de déclenchement des alarmes dans la Recommandation UIT-T X.736.

7.6.2 Fonction d'enregistrement d'audit de sécurité

Un enregistrement d'audit de sécurité est utilisé pour enregistrer les événements relatifs à la sécurité et, en particulier, les violations de sécurité. Parmi les événements relatifs à la sécurité, on peut citer les connexions, les déconnexions, les utilisations de mécanismes de sécurité, les opérations de gestion et la comptabilisation de l'utilisation. La *fonction d'enregistrement d'audit de sécurité* est définie dans la Recommandation UIT-T X.740.

7.6.3 Contrôle d'accès pour les entités gérées

La Recommandation UIT-T X.741 définit de façon très détaillée le modèle associé à l'attribution d'un certain contrôle d'accès aux diverses entités gérées. Cette Recommandation permet notamment de satisfaire aux exigences suivantes: protéger les informations de gestion contre toute création, suppression et modification non autorisées, faire en sorte que les opérations soient compatibles avec les droits d'accès de ceux qui sont à l'origine des opérations et empêcher la transmission d'informations de gestion à des destinataires non autorisés. Divers niveaux de contrôle d'accès sont définis pour respecter ces exigences. Pour les opérations de gestion, des restrictions d'accès peuvent être appliquées à plusieurs niveaux. Une politique de contrôle d'accès peut être fondée sur un ou plusieurs des mécanismes définis (par exemple, les listes de contrôle d'accès; les contrôles d'accès fondés sur des capacités, des étiquettes et des contextes). Dans le modèle défini dans la Recommandation UIT-T X.741, la décision de permettre ou de refuser l'accès est fondée sur la politique de contrôle d'accès et sur les informations de contrôle d'accès (ACI, *access control information*). Les informations ACI sont par exemple constituées de règles, de l'identité du demandeur, des identités des cibles auxquelles l'accès est demandé et d'informations relatives à l'authentification du demandeur.

7.6.4 Services de sécurité fondés sur l'architecture CORBA

Tandis qu'un grand nombre des Recommandations UIT-T de la série X.700 reposent sur l'utilisation du protocole CMIP comme protocole aux interfaces de gestion, il existe d'autres tendances qui sont maintenant prises en compte dans ces Recommandations, en particulier l'utilisation d'un protocole, de services et de modèles d'objet fondés sur l'architecture de courtier commun de requêtes d'objets (CORBA) pour les interfaces de gestion. Il convient notamment de citer les Recommandations UIT-T X.780, UIT-T X.780.1, UIT-T X.780.2 et UIT-T X.781. De plus, la Recommandation UIT-T Q.816 définit un cadre pour l'utilisation de ces services dans le contexte des interfaces de gestion. En ce qui concerne la prise en charge des exigences de sécurité pour ces interfaces, la Recommandation UIT-T Q.816 renvoie à la spécification de l'OMG (*object management group*) relative aux services de sécurité communs.

8. Approches particulières relatives à la sécurité des réseaux

8 Approches particulières relatives à la sécurité des réseaux

Le présent Chapitre traite des approches utilisées pour protéger divers types de réseau. Il présente tout d'abord les exigences de sécurité pour les réseaux de prochaine génération, puis les réseaux de communications mobiles qui passent d'une mobilité fondée sur une seule technologie (comme CDMA ou GSM) à une mobilité à travers des plates-formes hétérogènes utilisant le protocole Internet (IP). Il expose ensuite les dispositions relatives à la sécurité pour les réseaux domestiques et la télévision par câble et, enfin, les problèmes de sécurité dans les réseaux de capteurs ubiquitaires.

8.1 Sécurité des réseaux de prochaine génération (NGN)

Un réseau de prochaine génération (NGN, *next generation network*) est un réseau en mode paquet qui est en mesure de fournir des services de télécommunication aux utilisateurs et d'utiliser de multiples technologies de transport à large bande à qualité de service imposée. De plus, les fonctions liées aux services sont indépendantes des technologies sous-jacentes liées au transport. Un réseau NGN permet aux utilisateurs d'accéder sans restriction aucune aux réseaux ainsi qu'aux services et fournisseurs de services concurrents. Il prend en charge la mobilité généralisée qui permet de fournir des services aux utilisateurs de façon stable et ubiquitaire. On trouvera plus de détails sur les caractéristiques générales d'un réseau NGN dans la Recommandation UIT-T Y.2001.

8.1.1 Objectifs et exigences de sécurité des réseaux NGN

La sécurité étant l'une des fonctionnalités qui caractérisent les réseaux NGN, il est essentiel de mettre en place un ensemble de normes qui garantiront, dans la mesure du possible, la sécurité des réseaux NGN. A mesure que les réseaux NGN évoluent et que de nouvelles vulnérabilités apparaissent sur le plan de la sécurité pour lesquelles il n'existe pas de solution automatique immédiate, ces vulnérabilités doivent être décrites correctement afin que les administrateurs de réseau et les utilisateurs finals puissent en limiter les effets.

La Recommandation UIT-T Y.2701, qui s'appuie sur les principes énoncés dans la Recommandation UIT-T X.805, énonce des exigences de sécurité pour protéger les réseaux NGN contre les menaces de sécurité et examine certains aspects techniques de la gestion d'identité.

Les éléments suivants doivent être protégés dans un environnement multiréseaux:

- l'infrastructure des fournisseurs de réseau et de service et les actifs (par exemple les actifs et les ressources des réseaux NGN tels que les éléments de réseau, les systèmes, les composants, les interfaces, les données et les informations), les ressources, les communications (à savoir le trafic de signalisation, de gestion et de données/support) et les services associés;

- les services et capacités des réseaux NGN (par exemple les services vocaux, vidéo et de données); et

- les communications des utilisateurs finals et les informations les concernant (par exemple les informations privées).

Les exigences doivent permettre d'assurer la sécurité des communications des utilisateurs finals à travers les domaines administratifs de plusieurs réseaux, comme le montre la Figure 22.

Les exigences définies dans la Recommandation UIT-T Y.2701 sont considérées comme un ensemble minimal d'exigences. Un fournisseur NGN devra peut-être prendre des mesures en plus de celles spécifiées.

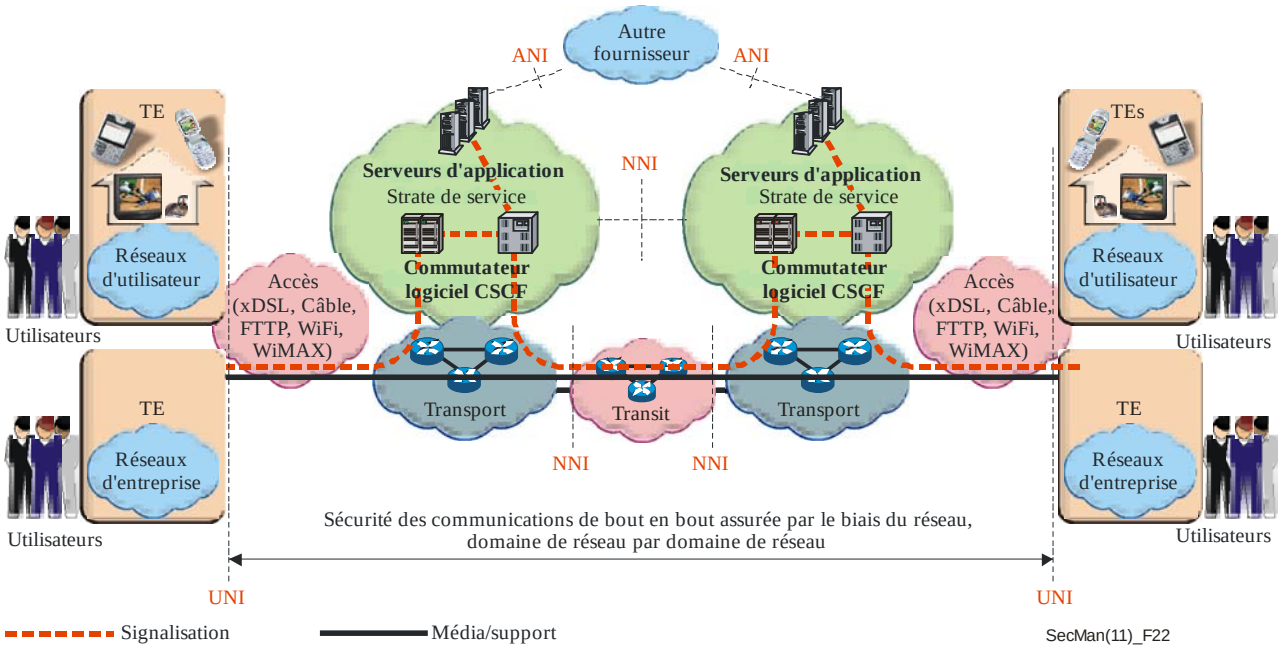


Figure 22 – Sécurité des communications à travers plusieurs réseaux

Outre les exigences spécifiées dans la Recommandation UIT-T Y.2701, la Recommandation UIT-T Y.2702 donne des exigences détaillées concernant l'authentification et l'autorisation pour les réseaux de prochaine génération, tandis que la Recommandation UIT-T Y.2704 définit les mécanismes de sécurité qui permettent de satisfaire aux exigences décrites dans les Recommandations UIT-T Y.2701 et UIT-T Y.2702.

La Recommandation UIT-T Y.2740 définit des exigences propres à la prise en charge dans les réseaux NGN des transactions financières à distance sur mobile.

8.2 Sécurité des communications mobiles

Pour les communications mobiles, on passe d'une mobilité se limitant à une technologie donnée (par exemple GSM ou CDMA) à une mobilité à travers des réseaux hétérogènes (par exemple GSM, Wi-Fi, RTPC) avec l'utilisation du protocole IP. Les réseaux futurs intégreront des réseaux sans fil et des réseaux filaires et offriront une large gamme de nouveaux services qui ne pouvaient pas être offerts par un seul et même réseau existant.

Avec le déploiement d'une vraie convergence fixe-mobile (FMC), un utilisateur mobile peut naviguer à travers plusieurs réseaux hétérogènes (par exemple GSM, LAN sans fil et Bluetooth). Les exigences de sécurité pour chaque type d'accès seront respectées de différentes manières mais toutes les exigences de sécurité doivent être respectées pour protéger les utilisateurs, les réseaux et les applications utilisées.

Parmi les problèmes de sécurité, on distingue d'une manière générale:

- les problèmes découlant de l'utilisation du protocole IP dans des réseaux mobiles sans fil; et
- les problèmes découlant de l'utilisation de plusieurs réseaux multi-technologies.

Les attaques et vulnérabilités sur l'Internet constituent une menace pour les réseaux mobiles sans fil qui utilisent le protocole IP comme protocole de transport. En outre, de nouvelles menaces découleront de la nature même des réseaux sans fil proprement dits, à savoir leur mobilité. Etant donné que les mécanismes de sécurité déjà élaborés pour les réseaux IP ne satisferont peut-être pas tous les besoins de sécurité des systèmes sans fil fondés sur IP, il faudra peut-être élaborer des mesures de sécurité IP nouvelles ou améliorées. Par ailleurs, la sécurité doit être prise en compte non seulement pour l'interface radioélectrique, mais aussi pour le service complet de bout en bout et elle doit être suffisamment souple pour offrir divers niveaux de sécurité adaptés au service ou à l'application qui est offert.

La multiplicité des réseaux augmente les risques de menaces telles que l'interception illégale de profils d'utilisateur, de contenus (par exemple communications vocales ou de données) et d'informations d'authentification. Par conséquent, le déploiement de services et d'applications IP mobiles nécessite la mise en œuvre de mesures de sécurité supplémentaires pour protéger l'utilisateur, l'opérateur et le fournisseur de services.

Les télécommunications mobiles internationales 2000 (IMT-2000) constituent la norme mondiale pour les communications sans fil de troisième génération (3G). Définies par un ensemble de Recommandations de l'UIT interdépendantes, les IMT-2000 offrent un cadre pour l'accès sans fil dans le monde entier grâce à l'interconnexion des divers systèmes de réseaux de Terre et/ou à satellite. Elles exploitent la synergie potentielle entre les technologies de télécommunications mobiles numériques et les systèmes d'accès sans fil fixes et mobiles.

Les activités de l'UIT sur les IMT-2000 concernent une normalisation internationale et portent sur l'attribution de bandes de fréquences et les spécifications techniques pour les composantes radio et réseau, la tarification et la facturation, l'assistance technique et les études sur les aspects réglementaires et politiques.

Les exigences générales de sécurité des réseaux IMT-2000 font l'objet des Recommendations UIT-T Q.1701, UIT-T Q.1702 et UIT-T Q.1703.

En outre, les spécifications 3G figurant dans les Recommandations UIT-T de la série Q.1741.x (3GPP) et de la série Q.1742.x (3GPP2) contiennent une évaluation des menaces perçues et une liste d'exigences de sécurité pour faire face à ces menaces. Ces Recommandations contiennent aussi des objectifs et des principes de sécurité pour les communications mobiles, la définition d'une architecture de sécurité, des exigences concernant les algorithmes cryptographiques, des exigences concernant l'interception licite ainsi que l'architecture et les fonctions de l'interception licite.

8.2.1 Communications mobiles sécurisées de données de bout en bout

Les terminaux mobiles dotés de capacités de communication de données (Wi-Fi, téléphones mobiles GSM, ordinateurs portables, tablettes portables, liseuses électroniques, PDA, etc.) sont très répandus et sont utilisés pour un nombre croissant d'applications. Du fait de la nature des réseaux sans fil et des vulnérabilités inhérentes aux technologies de communication sans fil, il est essentiel d'assurer efficacement la sécurité pour protéger à la fois les applications et les données.

La sécurité doit être prise en considération du point de vue de l'opérateur de réseau mobile, du fournisseur de service d'application et de l'utilisateur final. La sécurité entre le terminal mobile et le serveur d'application est particulièrement importante. En ce qui concerne les communications mobiles de bout en bout, l'UIT-T a élaboré un ensemble complet de solutions de sécurité, dont certaines sont examinées ci-dessous.

8.2.1.1 Cadre pour les communications mobiles sécurisées de données de bout en bout

La Recommandation UIT-T X.1121 décrit deux modèles de communications mobiles de données de bout en bout entre un utilisateur mobile et un fournisseur de service d'application (ASP, *application service provider*), à savoir un modèle général et un modèle avec passerelle (voir les Figures 23 et 24). Le service est fourni aux utilisateurs mobiles par l'intermédiaire du serveur d'application. Dans le modèle avec passerelle, la passerelle de sécurité sert de relais pour les paquets entre le terminal mobile et le serveur d'application et convertit un protocole de communication fondé sur le réseau mobile en un protocole fondé sur un réseau ouvert, et inversement. La Figure 25 décrit les menaces concernant le réseau de communications mobiles de données de bout en bout. La Figure 26 indique les endroits où des fonctions de sécurité sont nécessaires pour chaque entité et la relation entre les entités.

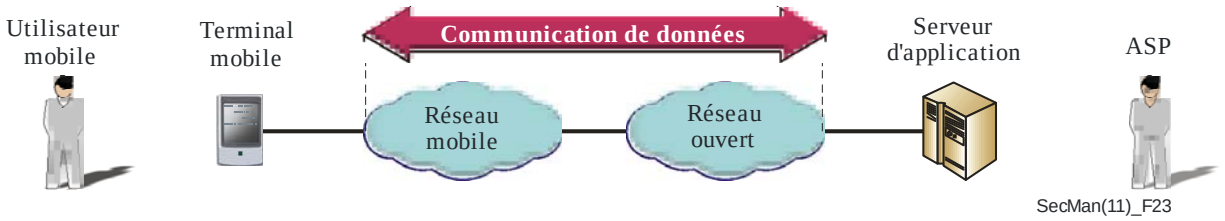


Figure 23 – Modèle général pour les communications de données de bout en bout entre un utilisateur et un ASP

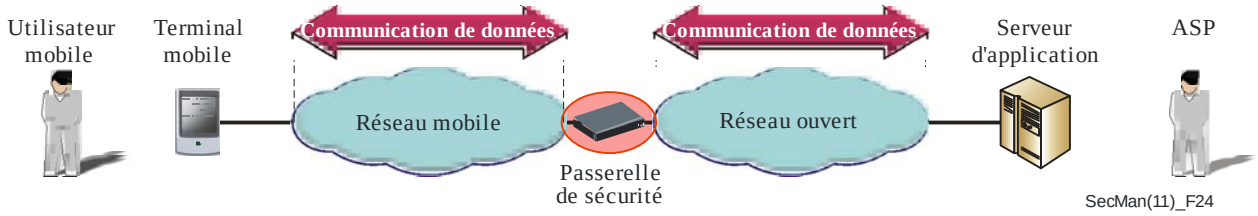


Figure 24 – Modèle avec passerelle pour les communications mobiles de données de bout en bout entre un utilisateur mobile et un ASP

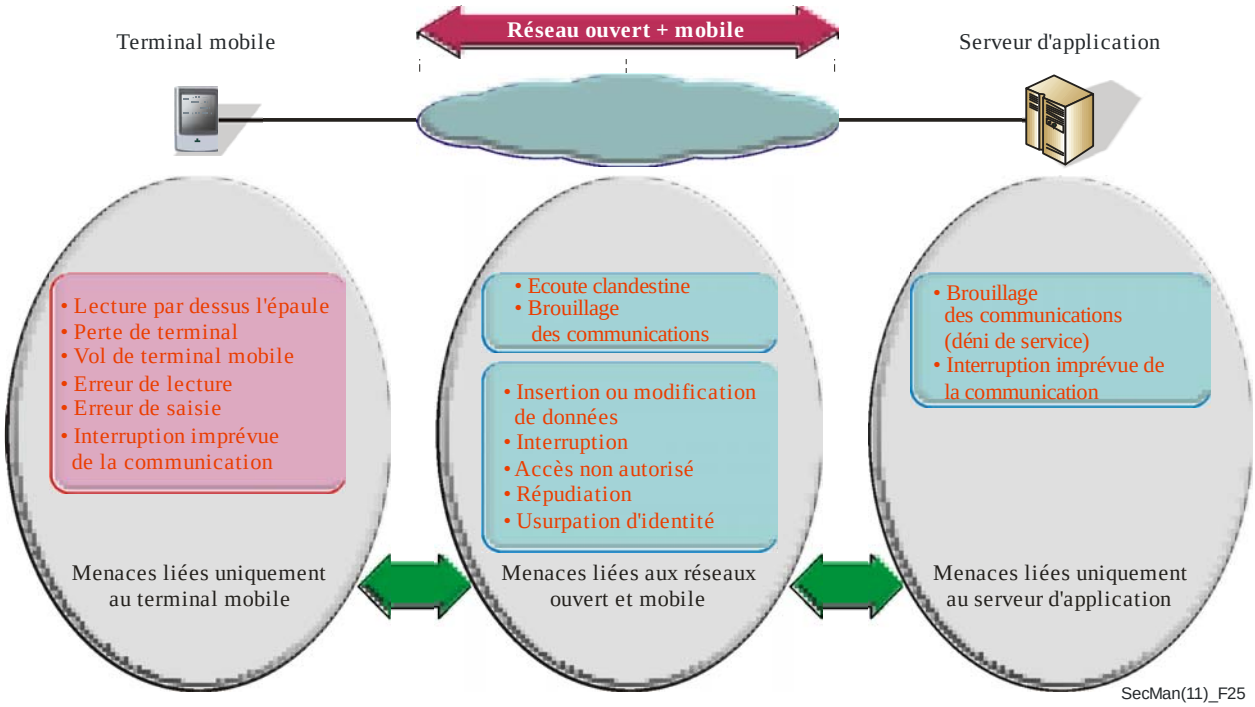


Figure 25 – Menaces concernant les communications mobiles de bout en bout

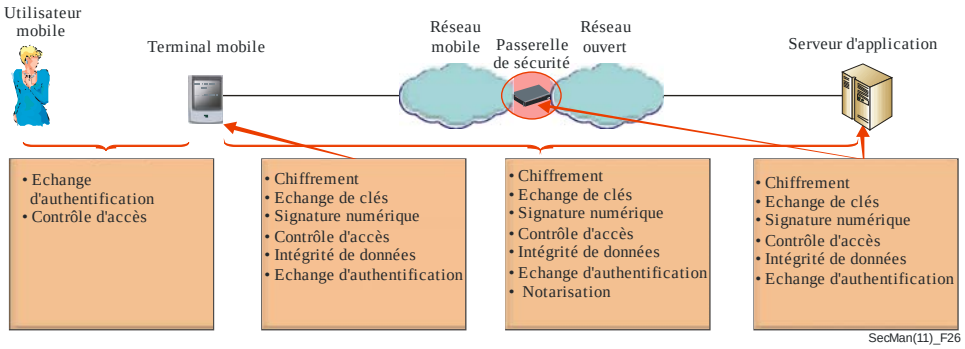


Figure 26 – Fonction de sécurité requise pour chaque entité et relation entre les entités

8.2.1.2 Infrastructure de clé publique (PKI) pour les communications mobiles sécurisées de données de bout en bout

L'infrastructure PKI est très utile pour la fourniture de certaines fonctions de sécurité (par exemple confidentialité, signature numérique, intégrité des données) nécessaires pour les communications mobiles de données de bout en bout, mais une certaine adaptation est nécessaire en raison des caractéristiques des communications mobiles de données. Des indications sur la mise en œuvre de l'infrastructure PKI dans un environnement mobile sont données dans la Recommandation UIT-T X.1122, qui décrit à la fois un modèle PKI général et un modèle PKI avec passerelle.

Dans le modèle général (illustré sur la Figure 27), une autorité de certification (CA, *certification authority*) fournit à l'utilisateur mobile un service de délivrance de certificat de l'utilisateur et de gestion du répertoire et de la liste de révocation de certificats (CRL, *certificate revocation list*). Une autorité de validation (VA, v*alidation authority*) fournit à l'utilisateur mobile un service de validation de certificat en ligne. L'autorité de certification utilisée par le fournisseur ASP délivre le certificat du fournisseur ASP et gère le répertoire et la liste CRL du fournisseur ASP. L'autorité de validation du fournisseur ASP assure un service de validation de certificat en ligne pour les certificats de fournisseur ASP.

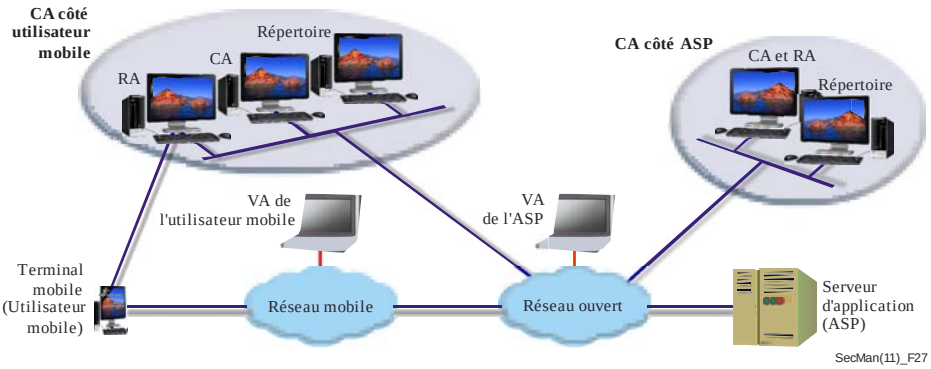


Figure 27 – Modèle PKI général pour les communications mobiles de données de bout en bout

Il existe deux méthodes de délivrance de certificat en fonction de l'endroit où les clés publique/privée sont générées. Dans la première méthode, la paire de clés de chiffrement générée et est produite au moment de la fabrication du terminal mobile; dans la deuxième méthode, la paire de clés de chiffrement est générée dans le terminal mobile ou dans un jeton infraudable rattaché au terminal mobile. La Figure 28 illustre la procédure d'acquisition d'un certificat par un terminal mobile, dans laquelle la paire de clés de chiffrement est générée dans le terminal mobile.

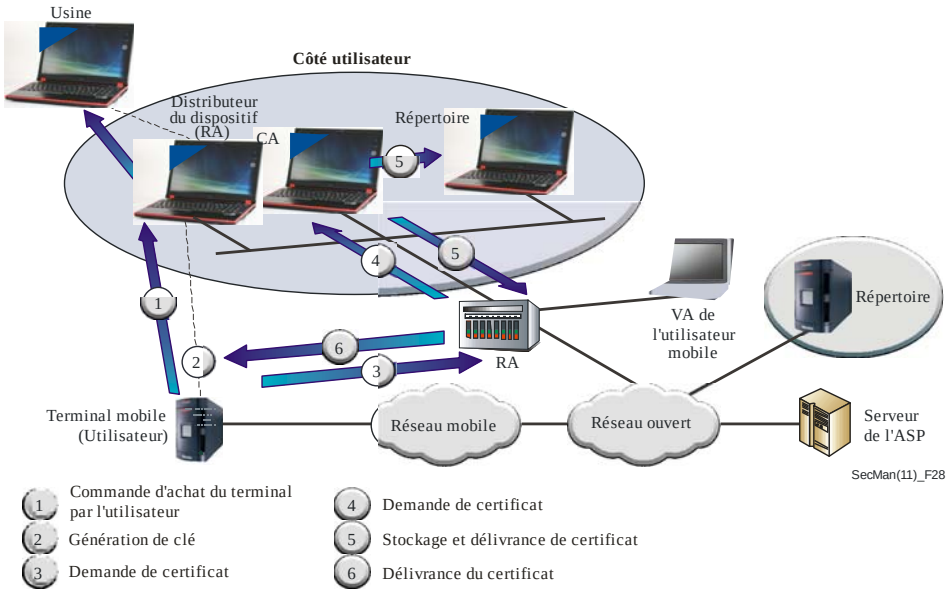


Figure 28 – Procédure de délivrance de certificat pour le terminal mobile

Le terminal mobile dispose souvent d'une puissance de calcul et d'une taille de mémoire limitées. Par conséquent, il est préférable de procéder à une validation de certificat en ligne plutôt qu'à une validation hors ligne sur la base d'une liste CRL. La Figure 29 illustre la procédure de validation de certificat en ligne pour un terminal mobile.

L'infrastructure PKI pour les communications mobiles de bout en bout peut être utilisée soit au niveau de la couche session, où elle peut prendre en charge des services de sécurité (par exemple, services d'authentification de client, d'authentification de serveur, de confidentialité et d'intégrité), soit au niveau de la couche application, où elle peut prendre en charge des services de non-répudiation et de confidentialité.

8.2.1.3 Système de réaction corrélative pour les communications mobiles de données

Le système de réaction corrélative a été conçu pour permettre aux terminaux ou dispositifs mobiles et au réseau de coopérer dans la lutte contre les menaces de sécurité. La Recommandation UIT-T X.1125 décrit l'architecture générique d'un système de réaction corrélative dans lequel un réseau mobile et ses terminaux d'utilisateur peuvent interagir afin de combattre diverses menaces concernant la sécurité des communications sécurisées de données de bout en bout. Ces menaces sont par exemple les virus, vers, chevaux de Troie ou d'autres menaces de réseau pesant à la fois sur le réseau mobile et sur ses utilisateurs.

Cette architecture offre aux réseaux des opérateurs une capacité de sécurité améliorée grâce à des mises à jour de sécurité dans les stations mobiles, un contrôle d'accès au réseau et des restrictions relatives aux services d'application. On établit aussi un mécanisme qui empêche les virus ou les vers de se propager rapidement dans le réseau de l'opérateur.

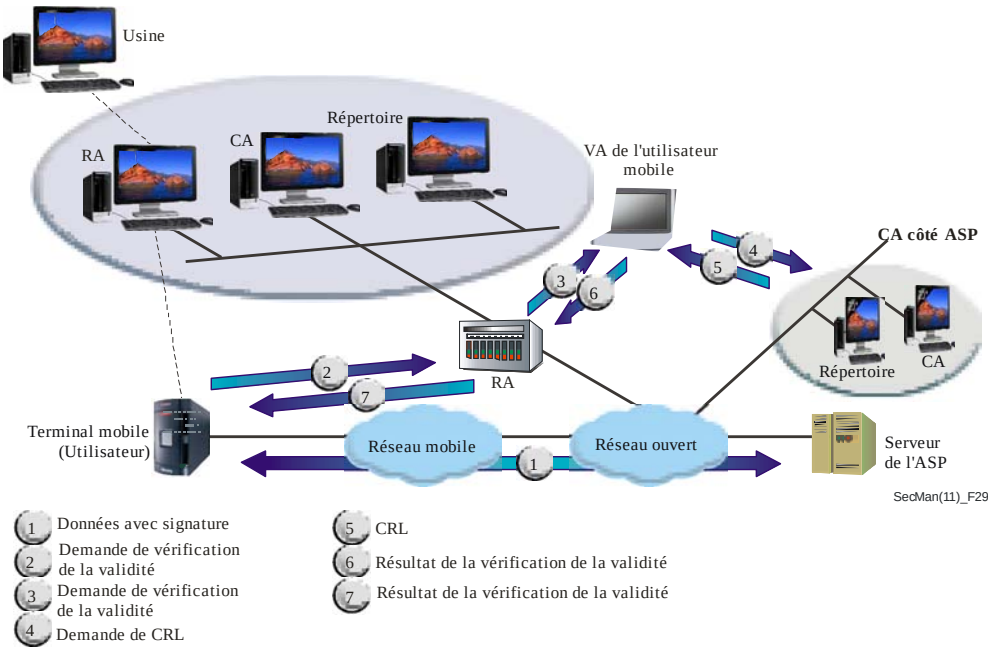


Figure 29 – Validation de certificat pour les communications mobiles de données de bout en bout

8.2.1.4 Transactions financières sécurisées sur mobile

L'architecture générale d'une solution de sécurité applicable au commerce sur mobile et aux services bancaires sur mobile dans le contexte des réseaux NGN fait l'objet de la Recommandation UIT-T Y.2741, qui décrit les principaux participants et leurs rôles, ainsi que les scénarios de fonctionnement des systèmes de commerce sur mobile et de services bancaires sur mobile. Cette Recommandation contient également des exemples de modèles de mise en œuvre des systèmes de commerce sur mobile et de services bancaires sur mobile.

8.3 Sécurité des réseaux domestiques

Etant donné qu'ils utilisent diverses techniques de transmission avec ou sans fil, les réseaux domestiques sont exposés à des menaces analogues à celles qui pèsent sur les autres réseaux. L'UIT-T a élaboré un ensemble complet de solutions pour protéger les services de réseau domestique, dont certaines sont examinées ci-après.

8.3.1 Cadre de sécurité pour les réseaux domestiques

La Recommandation UIT-T X.1111 s'appuie sur le modèle de menaces décrit dans la Recommandation UIT-T X.1121 pour établir un cadre de sécurité pour les réseaux domestiques. Les caractéristiques du réseau domestique peuvent être résumées comme suit:

- divers supports de transmission peuvent être utilisés dans le réseau;
- le réseau peut utiliser des technologies filaires et/ou sans fil;
- il existe de nombreux environnements possibles à prendre en considération du point de vue de la sécurité;
- des utilisateurs à distance peuvent transporter avec eux des terminaux; et
- chaque type de dispositif de réseau domestique nécessite des niveaux de sécurité différents.

Le modèle général de réseau domestique pour la sécurité, qui est illustré sur la Figure 30, peut comprendre de nombreux dispositifs (PDA, PC et téléviseur/magnétoscope par exemple). Dans ce modèle, les dispositifs domestiques sont classés en trois types:

- les dispositifs de type A (télécommandes, PC ou PDA par exemple), qui ont la capacité de commander un dispositif de type B ou de type C;
- les dispositifs de type B qui sont des ponts connectant des dispositifs de type C (qui n'ont pas d'interface de communication) au réseau. Un dispositif de type B communique avec d'autres dispositifs du réseau grâce à un langage propriétaire ou à un mécanisme de commande; et
- les dispositifs de type C (caméras de sécurité, dispositifs audio/vidéo par exemple), qui fournissent un service aux autres dispositifs.

Certains dispositifs combinent les fonctions de type A et de type C.

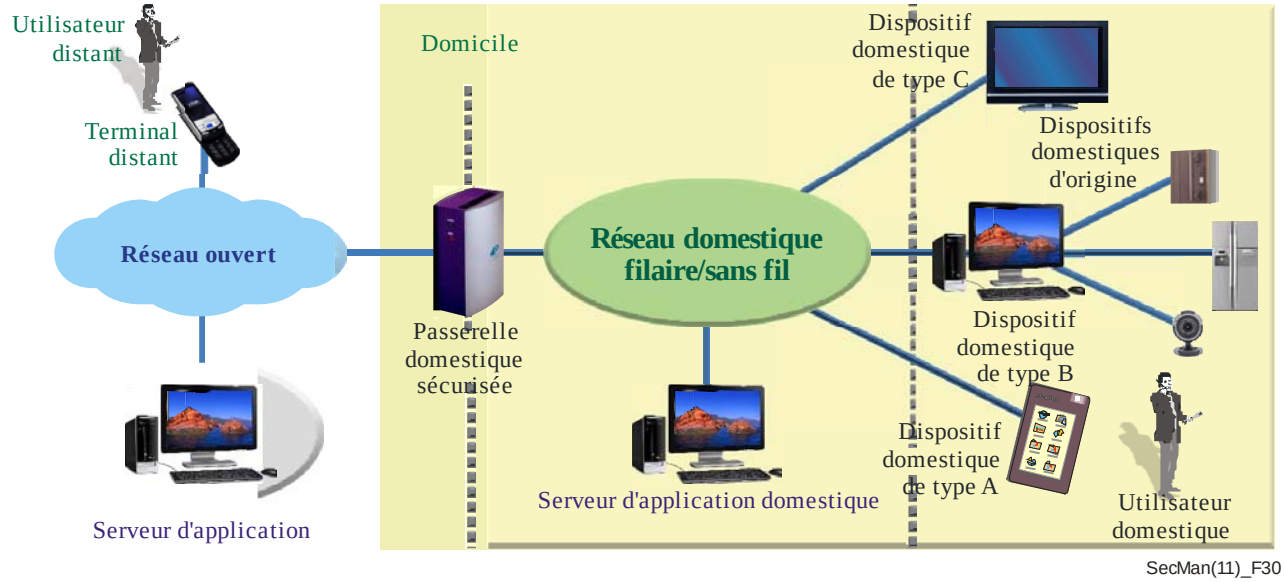


Figure 30 – Modèle général de réseau domestique pour la sécurité

La Recommandation UIT-T X.1111 décrit les menaces et les exigences en matière de sécurité du point de vue de l'utilisateur domestique et de l'utilisateur distant. De plus, elle classe les technologies de sécurité selon les fonctions satisfaisant aux exigences de sécurité et selon l'endroit où ces technologies doivent être appliquées.

8.3.2 Certification et authentification de dispositif dans les réseaux domestiques

Il existe deux options pour la certification de dispositif dans le réseau domestique: le modèle de délivrance externe, dans lequel tous les certificats de dispositif domestique sont délivrés par une autorité de certification (CA) externe, et le modèle de délivrance interne, dans lequel les certificats de dispositif (y compris les certificats; autosignés et les certificats d'entité finale) sont délivrés par une autorité de certification interne au réseau domestique. En règle générale, une autorité de certification interne est une passerelle domestique sécurisée capable de générer une paire de clés et de délivrer un certificat; autrement dit, la passerelle domestique peut délivrer à la fois un certificat d'autorité de certification et des certificats de dispositif domestique. La passerelle domestique sécurisée proprement dite peut avoir un certificat de dispositif qui est délivré par une autorité de certification externe et sera utilisé dans des services externes. Ce certificat de dispositif de passerelle domestique délivré en externe peut être utilisé pour l'authentification entre la passerelle domestique et le fournisseur de service de réseau.

La Recommandation UIT-T X.1112 décrit un cadre pour le modèle interne de délivrance, de gestion et d'utilisation de certificat de dispositif pour les réseaux domestiques. Ce modèle fait l'objet de la Figure 31.

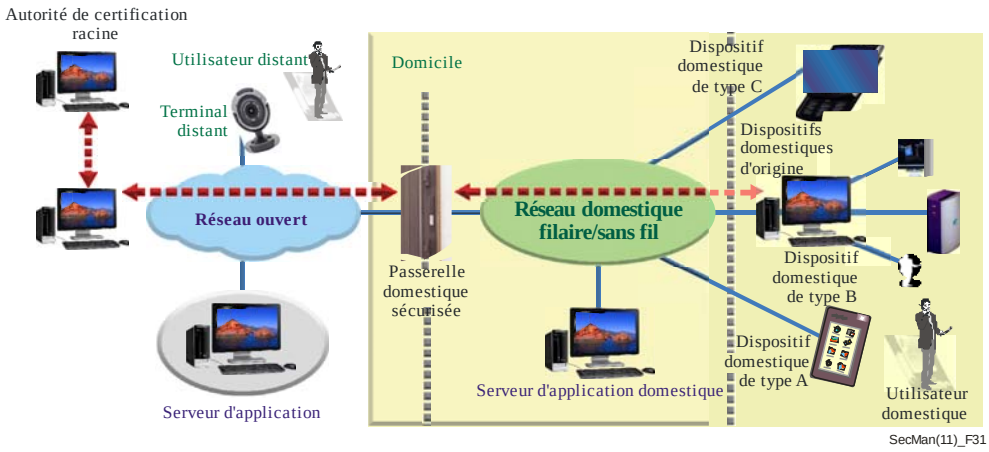


Figure 31 – Modèle d'authentification de dispositif pour réseau domestique sécurisé

Pour l'authentification de dispositif, un identificateur unique est nécessaire pour chaque dispositif du réseau domestique. Plus précisément, un certificat de dispositif domestique sera nécessaire en tant qu'élément de confiance unique lorsque le dispositif est utilisé dans le réseau domestique.

La Figure 32 montre quatre cas d'utilisation types d'un certificat de dispositif: 1) entre le terminal distant et la passerelle domestique sécurisée; 2) entre le serveur d'application et la passerelle domestique sécurisée; 3) entre les dispositifs domestiques et la passerelle domestique sécurisée; et 4) entre deux dispositifs domestiques.

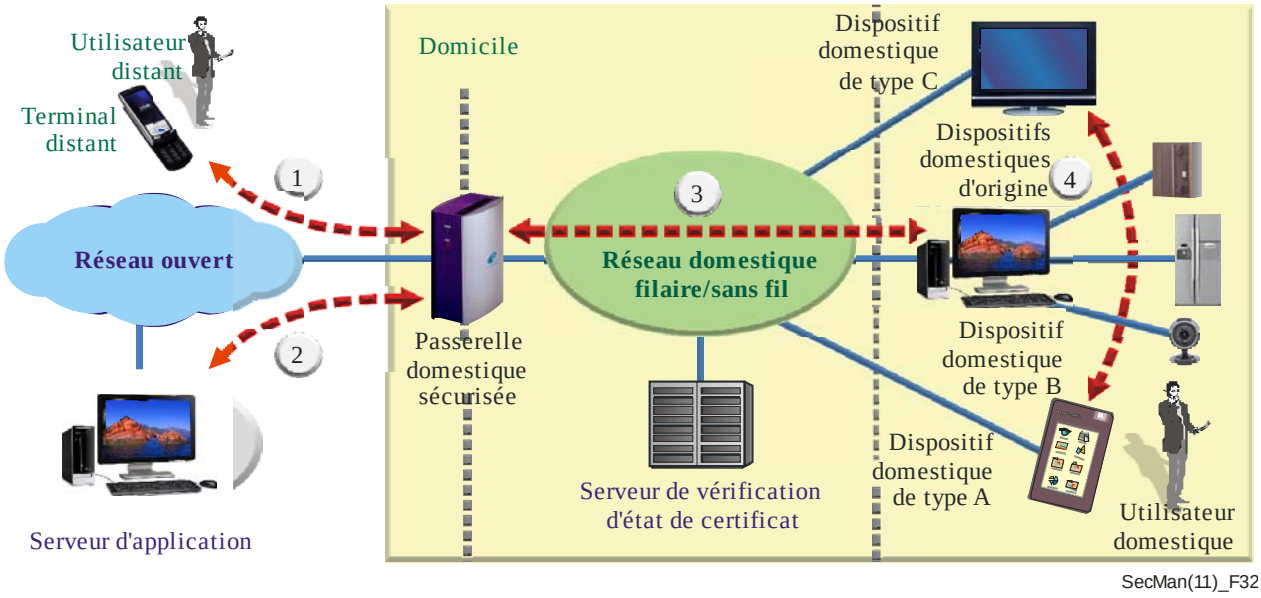


Figure 32 – Cas d'utilisation de l'authentification de dispositif basés sur le modèle général de réseau domestique pour la sécurité

Pour un service Internet externe entre le dispositif domestique et un serveur d'application externe, le dispositif domestique doit d'abord s'authentifier auprès de la passerelle domestique sécurisée en utilisant son propre certificat de dispositif. La passerelle domestique sécurisée doit ensuite s'authentifier auprès du serveur d'application externe en utilisant le certificat de passerelle domestique délivré par une autorité de certification externe. Ces cas d'utilisation peuvent être appliqués à divers protocoles d'application pour la prise en charge de services de réseau domestique sécurisés.

8.3.3 Authentification des utilisateurs humains pour les services de réseau domestique

Certains environnements exigent l'authentification de l'utilisateur humain et non d'un processus ou d'un dispositif. La Recommandation UIT-T X.1113 donne des indications sur l'authentification d'utilisateur dans les réseaux domestiques afin de permettre l'utilisation de différentes techniques d'authentification (par exemple, mots de passe, certificats et données biométriques). Elle définit également le niveau de garantie de sécurité et le modèle d'authentification suivant les scénarios de service d'authentification. La Figure 33 représente les flux de service d'authentification sur la base du modèle général de sécurité du réseau domestique défini dans la Recommandation UIT-T X.1111. Dans cet exemple, un utilisateur distant essaie d'accéder à des entités situées à l'intérieur du domicile, tandis que l'utilisateur domestique essaie d'accéder à des entités situées à l'intérieur ou à l'extérieur du domicile.

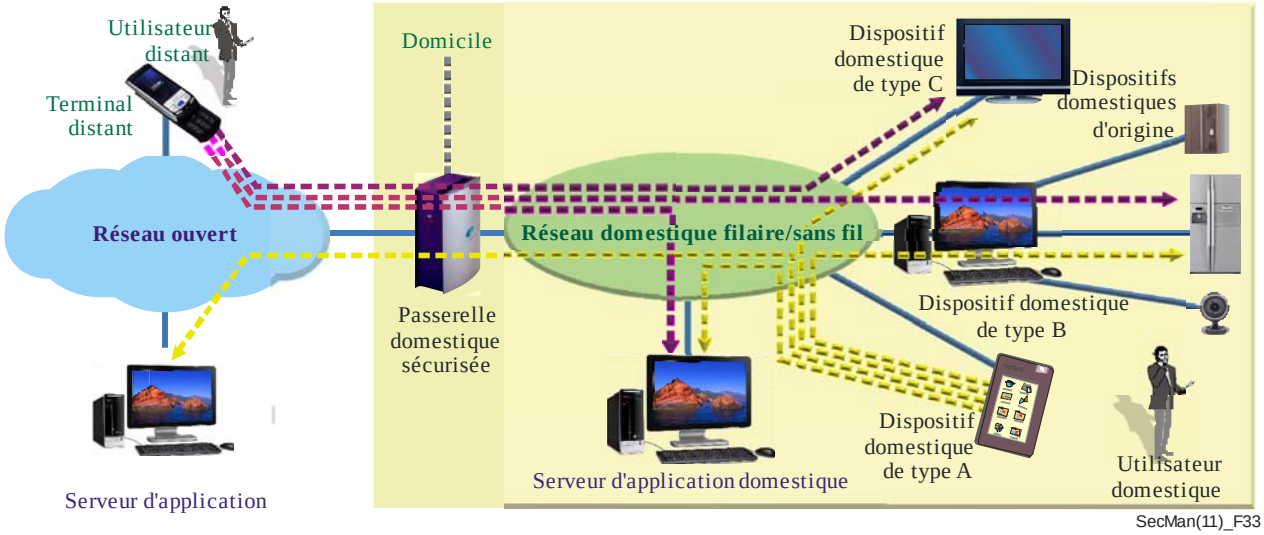


Figure 33 – Flux de service d'authentification pour le réseau domestique

8.4 IPCablecom

Le système IPCablecom permet aux opérateurs de télévision par câble d'offrir des services en temps réel fondés sur IP (par exemple des communications téléphoniques) sur des réseaux qui ont été améliorés pour prendre en charge des câblo-modems.

8.4.1 Architecture IPCablecom

L'architecture IPCablecom est définie dans la Recommandation UIT-T J.160. Les composants IPCablecom sont illustrés sur la Figure 34. L'architecture IPCablecom contient à la fois des éléments de réseau de confiance et des éléments de réseau non fiables. Normalement, les éléments de réseau de confiance sont situés à l'intérieur d'un réseau dorsal géré par un câblo-opérateur. Les éléments de réseau non fiables, comme les câblo-modems et les adaptateurs de terminal média (MTA, *media terminal adapter*), sont généralement situés en dehors des installations du câblo-opérateur, chez l'abonné.

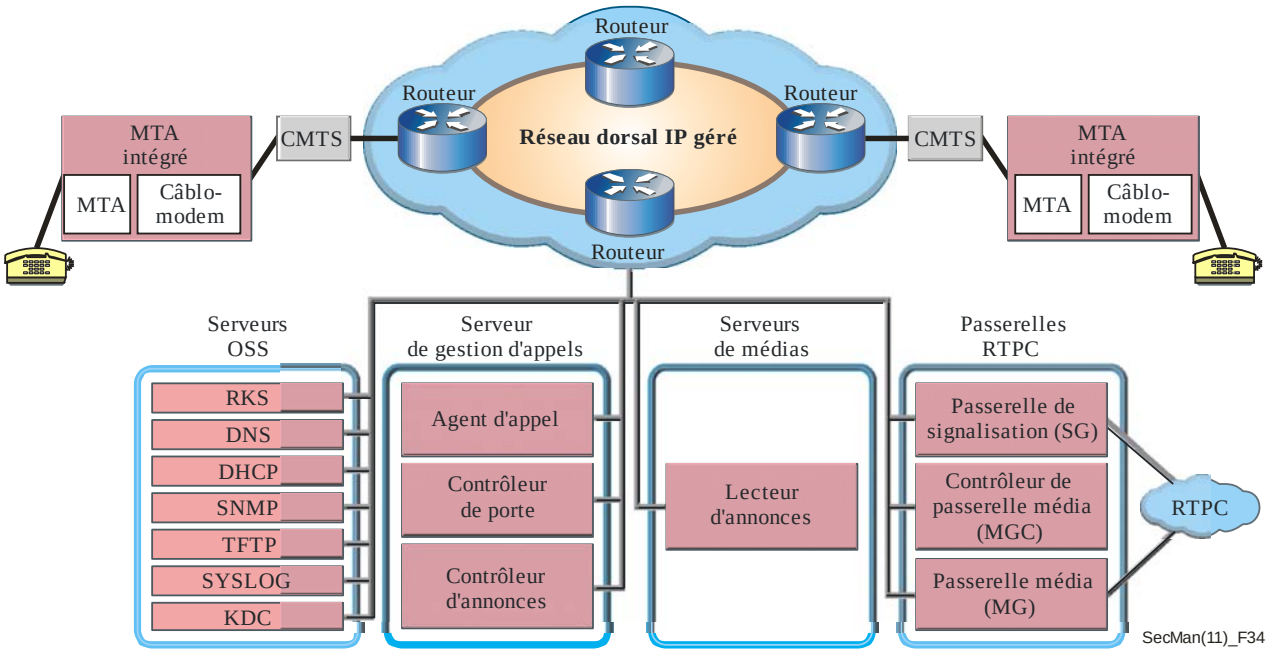


Figure 34 – Modèle de référence des composants IPCablecom

8.4.2 Exigences de sécurité pour IPCablecom

Chacune des interfaces de protocole IPCablecom est exposée à des menaces qui peuvent affecter à la fois l'abonné et le fournisseur de services. Par exemple, le trajet du flux de média peut passer par un grand nombre de fournisseurs de service Internet et de réseau dorsal potentiellement inconnus. Le flux de média peut alors être vulnérable aux écoutes clandestines, lesquelles entraînent une perte de la confidentialité des communications. Les objectifs de conception de la sécurité identifiés dans l'architecture IPCablecom sont les suivants:

- permettre des capacités vocales résidentielles avec au moins le même niveau perçu de confidentialité que dans le cas du RTPC;
- assurer une protection contre les attaques visant les adaptateurs MTA; et
- assurer une protection du câblo-opérateur contre les interruptions de réseau et les attaques par déni de service ou par vol de service.

Pour la conception, il faut prendre en compte la confidentialité, l'authentification, l'intégrité et le contrôle d'accès.

Les exigences de sécurité sont énoncées dans la Recommandation UIT-T J.170. Les menaces à prendre en compte sont récapitulées ci-dessous:

- vol de service, qui comprend la fraude à l'abonnement, le non-paiement de services, les clones d'adaptateur MTA (par exemple lorsqu'un adaptateur MTA enregistré sous un compte frauduleux est cloné), l'usurpation de l'identité d'un serveur de réseau et la manipulation de protocole;
- divulgation d'informations de canal support, qui comprend le simple espionnage, les clones d'adaptateur MTA (par exemple d'un adaptateur MTA accessible par le grand public), la manipulation de protocole, l'analyse cryptographique hors ligne et l'interruption de service;

- divulgation d'informations de signalisation;
- vol de services fondés sur les adaptateurs MTA; et
- enregistrement illégal d'un adaptateur MTA loué auprès d'un fournisseur de services différent.

8.4.3 Services et mécanismes de sécurité dans IPCablecom

Dans le système IPCablecom, la sécurité est mise en oeuvre dans les éléments les plus bas de la pile et utilise 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.

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. 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.

8.5 IPCablecom2

IPCablecom2 est une initiative du secteur du câble destinée à favoriser la convergence des technologies vocales, vidéo, de données et de mobilité.

8.5.1 Architecture IPCablecom2

IPCablecom2 est fondé sur la version 6 du sous-système multimédia IP (IMS, *IP multimedia subsystem*) définie dans le cadre du projet de partenariat pour la troisième génération (3GPP). Le 3GPP a notamment pour objet d'élaborer une architecture de communications IP fondées sur le protocole SIP pour les réseaux mobiles. L'architecture ainsi mise au point constitue la base de l'architecture IPCablecom2 définie dans la Recommandation UIT-T J.360.

8.5.2 Exigences de sécurité pour IPCablecom2

Les objectifs de conception pour l'architecture de sécurité IPCablecom2 sont les suivants:

- prise en charge des mécanismes permettant d'assurer la confidentialité, l'authentification, l'intégrité et le contrôle d'accès;
- protection du réseau contre les attaques par déni de service, interruption du réseau et vol de service;
- protection des équipements d'utilisateur (UE) (c'est-à-dire des clients) contre les attaques par déni de service, les failles de sécurité et l'accès non autorisé depuis le réseau;
- prise en charge du respect de la vie privée de l'utilisateur final par l'intermédiaire du chiffrement et de mécanismes de contrôle d'accès aux données de l'abonné telles que les informations de présence;
- mécanismes d'authentification des dispositifs, des équipements d'utilisateur et des utilisateurs ainsi que de mise en service, de signalisation et de téléchargement logiciel sécurisés;

- capacité de tirer parti et d'étendre l'architecture pour atteindre les objectifs précités.

Les menaces générales contre la sécurité d'IPCablecom2 sont les suivantes:

Menaces concernant le domaine de confiance

Un domaine de confiance est un groupement logique d'éléments de réseau qui sont sécurisés pour les communications. Les menaces liées au domaine de confiance concernent les interfaces qui connectent des éléments de réseau à l'intérieur d'un domaine, les interfaces entre domaines et les interfaces entre les équipements d'utilisateur et le fournisseur de services.

Vol de service

Le vol de service peut être réalisé de diverses manières, en particulier (la liste n'est pas exhaustive): manipulation d'équipement d'utilisateur; exploitation de faille de protocole, usurpation d'identité, clonage d'équipement d'utilisateur (imitation d'un équipement d'utilisateur légitime), fraude à l'abonnement et non-paiement de services.

Interruption et déni de service

On peut citer les attaques générales par déni de service, les attaques par inondation (qui rendent indisponible un élément de réseau particulier, généralement en dirigeant une quantité excessive de trafic de réseau vers ses interfaces) et les attaques utilisant des zombies (systèmes de point d'extrémité compromis).

Menaces contre le canal de signalisation

Les attaques contre le canal de signalisation sont les suivantes: confidentialité compromise des informations de signalisation, attaques par intercepteur résultant de l'interception et de la modification possible du trafic transitant entre deux parties qui communiquent entre elles et attaques par déni de service dans le canal de signalisation.

Menaces contre le canal support

Les menaces contre le canal support concernent le trafic média transféré entre les parties qui communiquent entre elles.

Menaces de sécurité propres au protocole

Il existe toute une variété de menaces contre chaque protocole multimédia.

8.5.3 Services et mécanismes de sécurité dans IPCablecom2

IPCablecom2 utilise largement la sécurité de couche transport et d'autres mécanismes utilisés dans le sous-système multimédia IP 3GPP (3GPP 23.002 v6.10.0, *Network Architecture*, décembre 2005). Les paragraphes qui suivent résument les améliorations apportées à l'architecture de sécurité IMS par IPCablecom2.

8.5.3.1 Authentification de l'utilisateur et de l'équipement d'utilisateur

L'architecture IPCablecom2 prend en charge les mécanismes d'authentification suivants:

- authentification et concordance de clés fondées sur le sous-système multimédia IP;
- authentification fondée sur le condensé SIP (protocole d'ouverture de session); et
- amorçage par certificat.

L'architecture prend en charge les équipements d'utilisateur ayant plusieurs justificatifs d'authentification. Par exemple, un équipement d'utilisateur peut avoir un certificat pour accéder à des services lorsqu'il est connecté à un réseau câblé, et une carte de circuit intégré universelle (UICC) pour accéder à des services lorsqu'il est connecté à un réseau cellulaire.

Un abonné peut avoir plusieurs justificatifs. Il peut avoir plusieurs équipements d'utilisateur, avec des capacités différentes liées à ces justificatifs. Par exemple, un abonné peut avoir un adaptateur MTA avec un certificat lorsqu'il est à son domicile, et un équipement d'utilisateur avec une carte UICC lorsqu'il est en déplacement.

8.5.3.2 Sécurité de la signalisation

IPCablecom2 ajoute la sécurité de couche transport (TLS, *transport layer security*) en tant qu'option pour la sécurité de la signalisation entre l'équipement d'utilisateur et la fonction proxy de commande de session d'appel. L'utilisation de TLS (telle qu'elle est définie dans le cadre du sous-système multimédia IP (IMS)) est facultative pour la sécurité de la signalisation.

8.6 Réseaux de capteurs ubiquitaires

Un capteur est simplement un dispositif qui produit un signal électrique qui représente une propriété physique mesurable. Un réseau de capteurs ubiquitaires (USN, *ubiquitous sensor network*) est un réseau qui utilise des capteurs à faible coût et à faible puissance pour connaître le contexte afin de fournir des services reposant sur les informations détectées et le savoir à tous les utilisateurs, quels que soient l'endroit et le moment. Un réseau USN peut couvrir une grande zone géographique et peut prendre en charge diverses applications. La Figure 35 illustre les applications potentielles des réseaux USN.

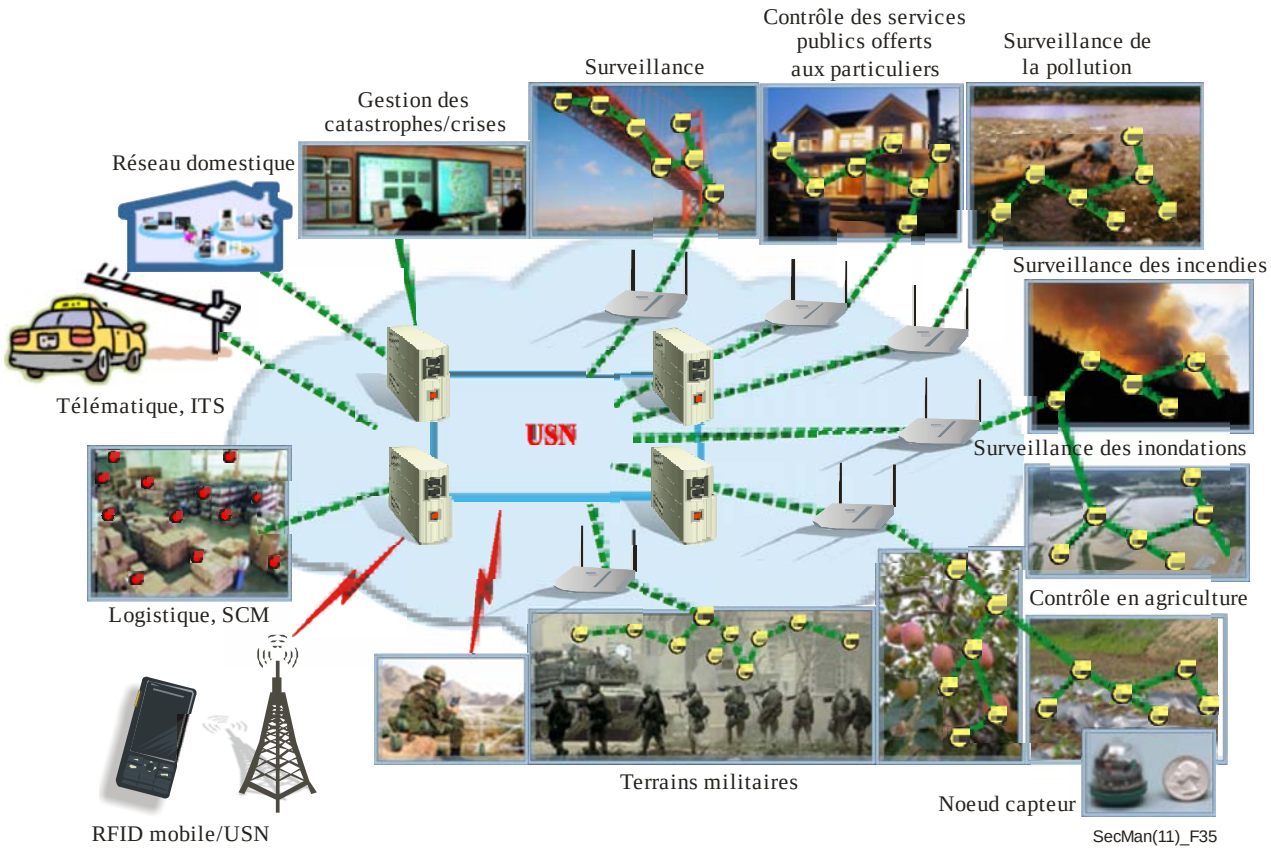


Figure 35 – Applications potentielles des réseaux USN

Les réseaux de capteurs sont généralement raccordés aux réseaux des utilisateurs finals et, même si les réseaux de transmission centraux utilisent souvent l'Internet et les technologies NGN, diverses technologies sous-jacentes (DSL, satellite, GPRS, CDMA, GSM, etc.) seront utilisées.

Etant donné que le transfert d'informations dans un réseau USN est exposé à de nombreuses menaces potentielles, des techniques de sécurité efficaces sont nécessaires pour lutter contre ces menaces.

8.6.1 Cadre de sécurité des réseaux de capteurs ubiquitaires

Les avancées réalisées récemment dans le domaine des technologies de communication sans fil et de l'électronique ont facilité la mise en œuvre de réseaux de capteurs ubiquitaires (USN, *ubiquitous sensor network*). Un réseau USN comprend trois principaux éléments: un réseau de capteurs composé d'un grand nombre de nœuds capteurs, une station de base (également appelée passerelle) qui fait office d'interface entre le réseau de capteurs et un serveur d'application et un serveur d'application qui commande les nœuds capteurs ou collecte les données détectées par les nœuds capteurs.

La Recommandation UIT-T X.1311 décrit les menaces pesant sur la sécurité des réseaux USN et les exigences de sécurité pour ces réseaux. En outre, elle clase les techniques de sécurité selon les fonctions qui satisfont aux exigences de sécurité et les points où les techniques de sécurité sont appliquées dans le modèle de sécurité USN.

La structure générale d'un réseau USN est présentée dans la Figure 36. Le domaine des réseaux de capteurs peut comprendre à la fois des réseaux de capteurs sans fil et des réseaux de capteurs filaires et un grand nombre de technologies de réseau filaires et sans fil peuvent être utilisées en fonction des caractéristiques et des exigences du service.

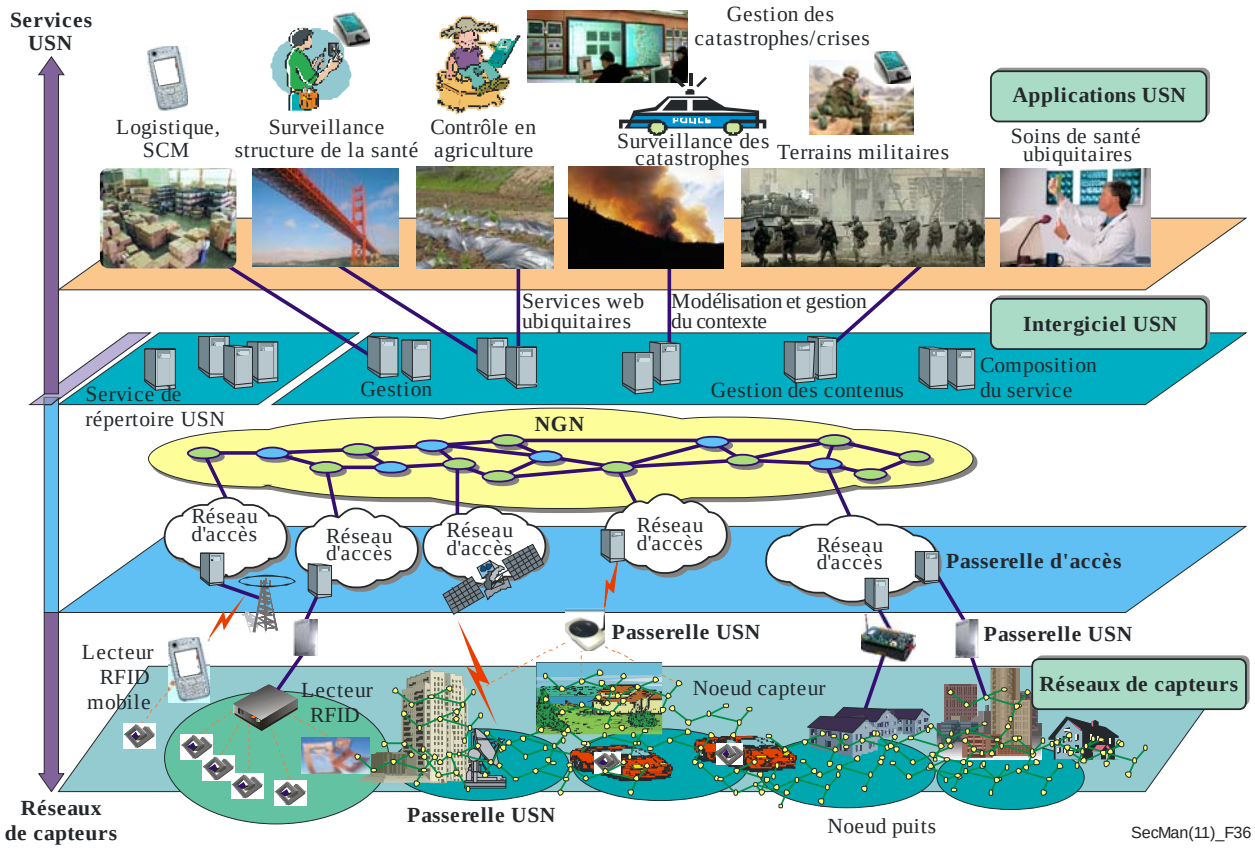


Figure 36 – Structure générale d'un réseau USN

Les réseaux USN sont notamment exposés aux mêmes menaces que les réseaux IP et les réseaux de capteurs. Il existe deux types de menaces pour les réseaux de capteurs: les menaces générales et les menaces liées au routage. Les Recommandations UIT-T X.800 et UIT-T X.805 (voir le Chapitre 4 et la Figure 1) recensent les menaces auxquelles les réseaux IP sont exposées et les menaces liées au routage pour l'échange de messages dans les réseaux de capteurs. En outre, certaines menaces sont propres aux nœuds capteurs (compromission des nœuds capteurs, écoutes clandestines, confidentialité des données détectées, attaque par déni de service et utilisation malveillante du réseau de base). Enfin, les sept autres menaces suivantes ont été identifiées:

- Usurpation, altération ou reproduction des informations de routage
- Retransmission sélective
- Attaques par siphon
- Attaques Sybil
- Attaques par trou de ver
- Attaques d'inondation par messages Hello
- Usurpation d'accusé de réception.

Le modèle de sécurité présenté dans la Figure 37 décrit un cadre général de sécurité des réseaux USN fondé sur le domaine d'application, la structure générale et la configuration des réseaux USN. Il s'appuie sur la norme ISO/CEI 15408-1 *Critères d'évaluation pour la sécurité TI* et vise à contribuer à mettre en place des concepts et des relations de sécurité pour les réseaux USN.

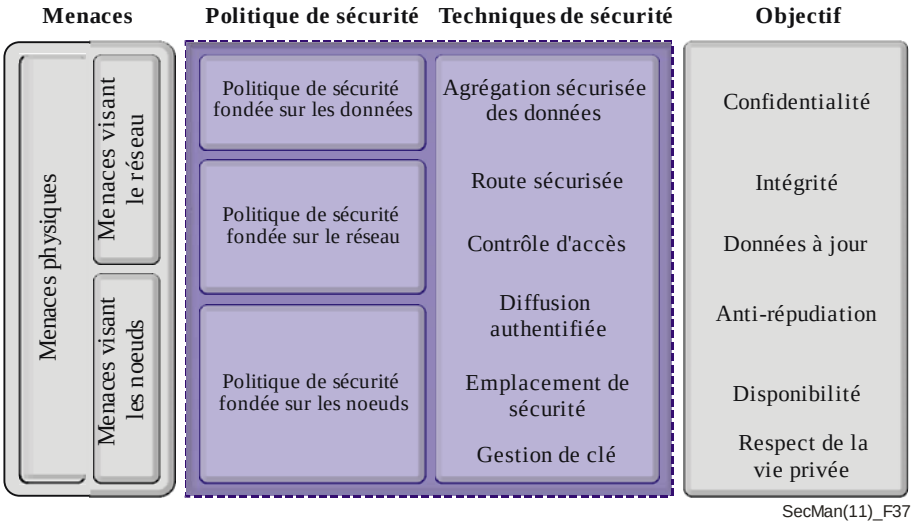


Figure 37 – Modèle de sécurité pour les réseaux USN

8.6.2 Intergiciels de réseaux de capteurs ubiquitaires (USN)

Un intergiciel de réseau USN est une entité intermédiaire qui fournit les fonctions dont ont habituellement besoin différents types d'applications et de services USN. Il reçoit les demandes des applications USN et transmet ces demandes aux réseaux de capteurs appropriés. De même, l'intergiciel USN reçoit des données brutes ou des données traitées envoyées par les réseaux de capteurs et les transmet aux applications USN appropriées. Il peut assurer des fonctions de traitement de l'information (traitement des requêtes, traitement en fonction du contexte, traitement des événements, surveillance du réseau de capteurs, etc.). La Recommandation UIT-T F.744 contient la description et les spécifications de service concernant les intergiciels USN, tandis que la Recommandation UIT-T X.1312 donne des lignes directrices sur la sécurité des intergiciels.

L'intergiciel USN est situé entre l'application USN et le réseau de capteurs dans le modèle de service USN. Les menaces auxquelles il est exposé sur le plan de la sécurité peuvent être subdivisées en trois groupes en fonction de la cible: dispositif, données et réseau.

Les menaces concernant la sécurité du système sont les suivantes: accès non autorisé à l'intergiciel USN, attaques par déni de service ou par déni de service réparti contre l'intergiciel USN, transfert de trafic malveillant ou anormal vers l'intergiciel USN, mauvaise utilisation ou utilisation abusive du système d'intergiciel USN, erreurs par négligence et rupture de confinement entre applications.

Les menaces concernant la sécurité des données sont la fuite et la falsification de données.

Les menaces concernant la sécurité des communications avec l'intergiciel sont les écoutes clandestines, l'interruption, le détournement et le brouillage.

Les exigences de sécurité pour les intergiciels USN doivent viser à éliminer chacune de ces menaces.

La Figure 38 illustre les fonctions de sécurité d'un intergiciel USN.

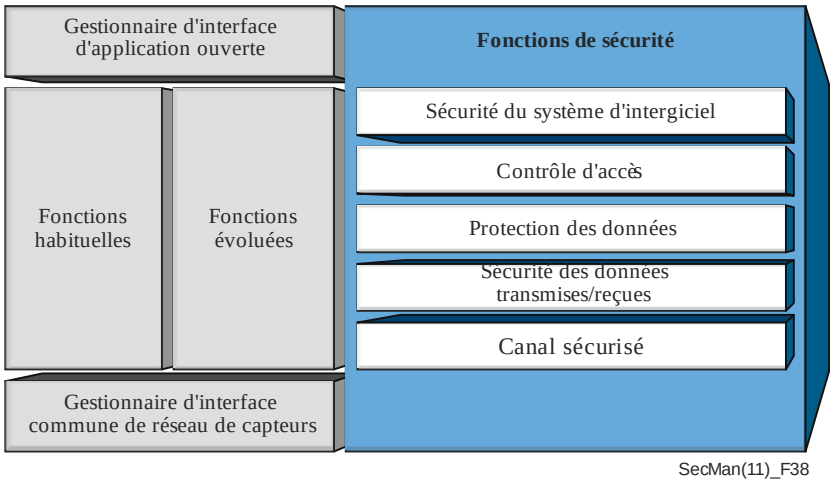


Figure 38 – Fonctions de sécurité d'un intergiciel USN

9. Cybersécurité et interventions en cas d'incident

9 Cybersécurité et interventions en cas d'incident

9.1 Partage et échange d'informations concernant la cybersécurité

Les cyberattaques sont fréquentes et occasionnent nombre de difficultés pour les utilisateurs, les fournisseurs de services et les opérateurs. Pour y faire face de façon efficace, il faut comprendre l'origine et la nature de l'attaque et échanger des informations avec les organismes de surveillance. La lutte contre les cyberattaques par des moyens techniques nécessite d'élaborer un cadre et des exigences permettant, d'une part, de détecter les cyberattaques, de se protéger contre elles, d'atténuer leurs effets et de permettre un retour à la normale après une cyberattaque et, d'autre part, de résoudre les problèmes techniques importants auxquels les opérateurs de réseau, les entreprises et les pouvoirs publics sont confrontés. L'UIT-T a déjà élaboré plusieurs Recommandations sur le partage efficace d'informations entre domaines en ce qui concerne la sécurité et les vulnérabilités et met actuellement au point des solutions pour prendre en charge la transparence en matière de télécommunication/TIC, les interventions en cas d'incident, la surveillance des menaces et l'évaluation des risques.

9.1.1 Echange d'informations sur la cybersécurité (CYBEX)

Les techniques CYBEX, qui font l'objet des Recommandations UIT-T de la série X.1500, visent à améliorer l'échange d'informations sur la cybersécurité tout en tenant compte du fait que les techniques en elles-mêmes et l'environnement dans lequel elles sont utilisées évoluent constamment.

Les techniques décrites dans les Recommandations "CYBEX" permettront aux organisations de télécommunication/TIC, y compris aux équipes d'intervention en cas d'incident informatique (CIRT, *computer incident response team*), au sein des juridictions et entre juridictions, de disposer des informations nécessaires pour faciliter des processus coopératifs sécurisés et des contrôles destinés à améliorer le niveau de garantie dans les échanges d'informations entre organisations et pour prendre des décisions, ce qui permet d'améliorer notablement la sécurité des installations et services de télécommunication/TIC dans le monde. En outre, ces Recommandations représentent une approche cohérente pour gérer et échanger des informations sur la cybersécurité à l'échelle mondiale et améliorent la sensibilisation à la sécurité et la collaboration afin d'atténuer les conséquences des cybermenaces, des cyberattaques et des logiciels malveillants.

9.1.2 Présentation générale de l'échange d'informations sur la cybersécurité

La Recommandation UIT-T X.1500 donne un modèle CYBEX et présente les techniques qui peuvent être utilisées pour faciliter les échanges d'informations sur la cybersécurité. Ces techniques peuvent être utilisées séparément ou de manière combinée, selon les souhaits ou les besoins, en vue d'améliorer la cybersécurité grâce à un échange d'informations cohérent, complet, global, garanti et en temps utile. Cette Recommandation n'impose aucune obligation quant à l'échange d'informations, et elle ne traite pas des moyens d'acquisition ou d'utilisation finale des informations. Ces techniques font appel à la découverte globale structurée et à l'interopérabilité d'informations sur la cybersécurité, afin de pouvoir s'adapter aux progrès constants accomplis dans le cadre des différents forums s'occupant de la cybersécurité.

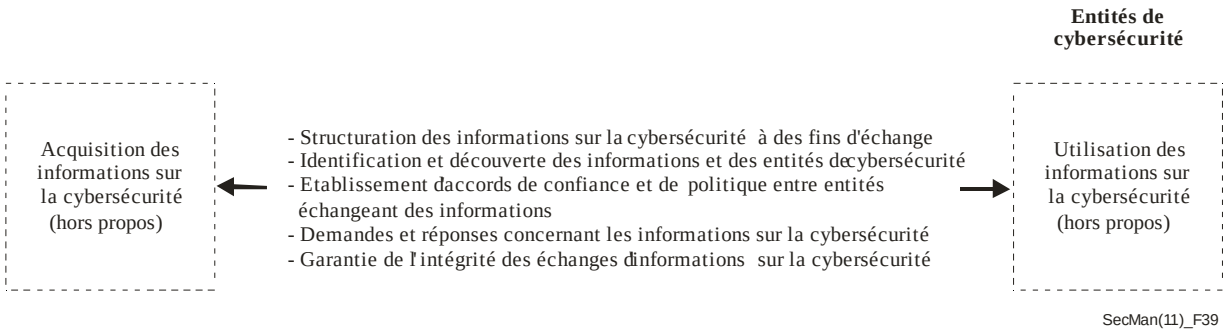


Figure 39 – Modèle CYBEX

Le modèle général d'échange d'informations sur la cybersécurité présenté dans la Figure 39 est composé de fonctions de base pouvant être utilisées séparément ou ensemble, selon qu'il conviendra, et étendues en fonction des besoins afin de faciliter les échanges d'informations sur la cybersécurité avec garanties. Ces fonctions sont les suivantes:

- structuration des informations sur la cybersécurité à des fins d'échange;
- identification et découverte d'informations et d'entités de cybersécurité;
- établissement d'accords de confiance et de politiques entre entités échangeant des informations;
- demandes et réponses concernant les informations sur la cybersécurité;
- garantie de l'intégrité des échanges d'informations sur la cybersécurité.

Dans les Recommandations UIT-T de la série X.1500, ces techniques sont en outre organisées en "grappes":

- failles, vulnérabilités et état;
- événement, incident et heuristique;
- politique d'échange d'informations;
- identification, découverte et interrogation;
- garantie d'identité;
- protocoles d'échange.

9.1.3 Echange d'informations sur les vulnérabilités

La Recommandation UIT-T X.1520 présente un moyen structuré d'échange d'informations sur les vulnérabilités et les expositions en matière de sécurité et donne un identificateur commun pour les problèmes connus du public. Elle définit l'utilisation des vulnérabilités et expositions courantes (CVE) pour faciliter l'échange de données entre des capacités distinctes (outils, répertoires et services) sur la base de cet identificateur commun. Elle vise à permettre l'utilisation conjointe de bases de données sur les vulnérabilités et d'autres capacités, d'une part, et à faciliter la comparaison des outils et services de sécurité, d'autre part. Le système CVE ne donne que le numéro d'identificateur standard avec un indicateur d'état, une brève description, et des références aux rapports et avertissements concernant la vulnérabilité en question (il ne

donne pas d'informations comme les risques, les incidences et les solutions, ni d'informations techniques détaillées).

L'objectif premier du système CVE est d'identifier les vulnérabilités et les expositions connues qui sont détectées par les outils de sécurité, ainsi que tout nouveau problème détecté.

9.1.4 Notation des vulnérabilités

La gestion des TIC doit permettre d'identifier et d'évaluer les vulnérabilités touchant de nombreuses plates-formes matérielles et logicielles disparates. Il faut ensuite classer ces vulnérabilités par ordre de priorité et remédier à celles qui présentent les plus grands risques. Etant donné que les vulnérabilités sont très nombreuses et que chacune est notée sur la base de différentes échelles, il incombe aux gestionnaires des TIC de déterminer comment les comparer et établir les priorités.

La Recommandation UIT-T X.1521 définit un cadre ouvert qui normalise les notes attribuées aux vulnérabilités, explique les propriétés et les différentes caractéristiques utilisées pour calculer une note et permet d'établir un ordre de priorité des risques en faisant en sorte que la note attribuée à une vulnérabilité soit représentative du risque réel par rapport à d'autres vulnérabilités.

Les paramètres utilisés dans le système de notation des vulnérabilités courantes (CVSS) sont répartis en trois groupes: paramètres de base, paramètres temporels et paramètres environnementaux (voir la Figure 40).

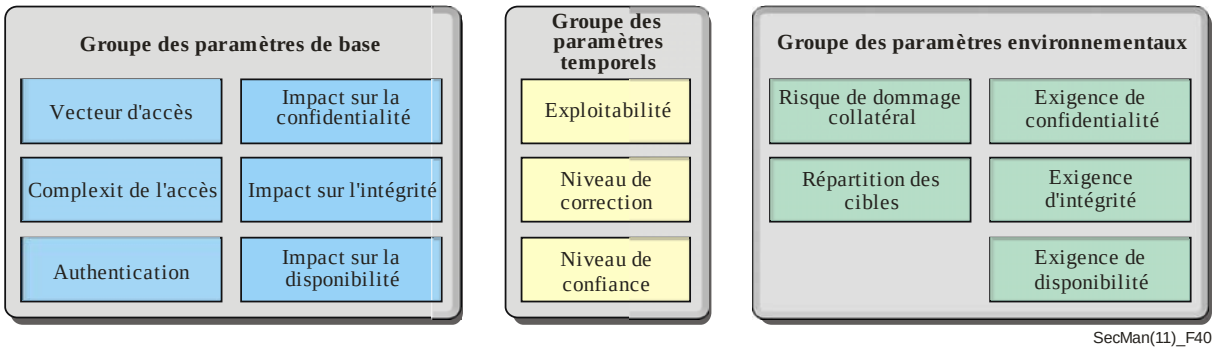


Figure 40 – Groupes de paramètres CVSS

Les paramètres de base représentent les caractéristiques intrinsèques et fondamentales d'une vulnérabilité qui sont constantes dans le temps et dans les environnements utilisateurs. Les paramètres temporels sont les caractéristiques d'une vulnérabilité qui évoluent dans le temps, mais d'un environnement utilisateur à l'autre. Enfin, les paramètres environnementaux sont les caractéristiques d'une vulnérabilité qui concernent un environnement utilisateur particulier et sont propres à cet environnement.

Le groupe de paramètres CVSS de base définit les caractéristiques fondamentales d'une vulnérabilité. Les utilisateurs ont ainsi une représentation claire et facile à comprendre d'une vulnérabilité. Ils peuvent alors invoquer les groupes de paramètres temporels et environnementaux pour fournir des informations contextuelles qui rendent compte de façon plus précise du risque pour leur propre environnement. Ils peuvent alors prendre des décisions en meilleure connaissance de cause lorsqu'ils essayent d'atténuer des risques liés à ces vulnérabilités.

Le système CVSS est utilisé de plusieurs façons différentes:

- Les fournisseurs de bulletins sur les vulnérabilités font figurer des notes pour les paramètres CVSS de base et temporels et des vecteurs dans leurs bulletins. Ces bulletins donnent de nombreuses informations, y compris la date de découverte, les systèmes affectés et les liens avec les fabricants pour des recommandations relatives à des correctifs.

- Les éditeurs d'applications logicielles informent leurs clients des notes pour les paramètres CVSS de base et des vecteurs pour les aider à comprendre la gravité des vulnérabilités dans leurs produits et, ainsi, à gérer plus efficacement leurs risques TIC.

- Les organisations d'utilisateurs utilisent le système CVSS en interne pour prendre des décisions en connaissance de cause en matière de gestion des vulnérabilités. Elles utilisent des scanners ou des technologies de contrôle pour localiser dans un premier temps les vulnérabilités concernant les serveurs et les applications. Elles combinent ces données avec les notes pour les paramètres CVSS de base, temporels et environnementaux pour obtenir davantage d'informations contextuelles sur les risques et éliminer les vulnérabilités qui représentent le plus grand risque pour leurs systèmes.

- Les organisations de gestion des vulnérabilités analysent les réseaux pour rechercher les vulnérabilités TIC. Elles donnent des notes pour les paramètres CVSS de base pour chaque vulnérabilité sur chaque serveur. Les organisations d'utilisateurs utilisent ensuite ces données pour gérer leurs activités relatives à la sécurité et se protéger contre des menaces intentionnelles ou accidentelles pesant sur les TIC.

- Les entreprises de gestion des risques liés à la sécurité utilisent les notes CVSS pour calculer le niveau de risque ou de menace dans une organisation. Lorsqu'elles sont utilisées avec des informations comme la topologie et les actifs du réseau, ces informations peuvent donner aux clients une vision plus juste de leur exposition aux risques.

- Le cadre ouvert qu'est le système CVSS permet aux chercheurs d'effectuer des analyses statistiques sur les vulnérabilités et leurs propriétés.

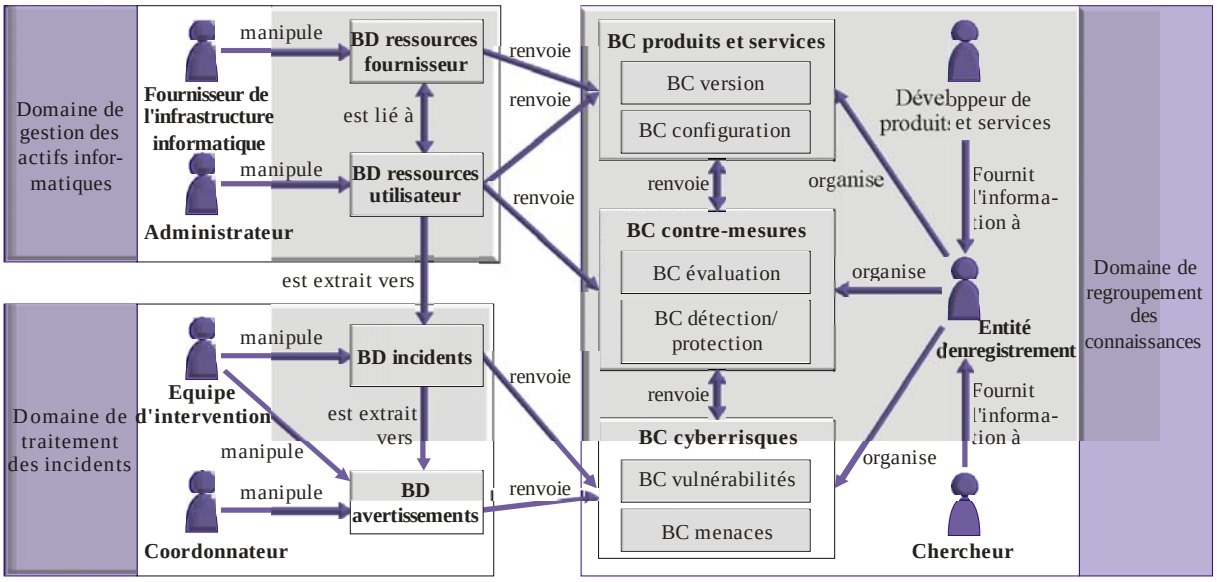
9.1.5 Découverte des informations de cybersécurité

La découverte des informations de cybersécurité fait appel à trois entités: une entité d'extraction, une source et un répertoire. L'entité d'extraction obtient des informations en envoyant une demande à la source, qui fournit les informations demandées. Le répertoire enregistre les métadonnées des informations fournies par la source et aide l'entité d'extraction à trouver une source appropriée.

La Recommandation UIT-T X.1570 décrit un cadre pour la découverte d'informations de cybersécurité et le mécanisme qui y est associé. Ce cadre couvre la façon de publier les informations sur la cybersécurité, d'obtenir la liste de sources possibles et d'acquérir les informations nécessaires.

Les mécanismes de découverte s'appuient sur des registres d'informations, qui peuvent être centralisés ou décentralisés. Lorsque les registres sont centralisés, on utilise le plus souvent un mécanisme de découverte fondé sur l'identificateur d'objet pour identifier et localiser les sources d'informations sur la cybersécurité. Dans le cas de registres répartis, la partie qui recherche l'information utilise un mécanisme de découverte fondé sur le cadre de description des ressources. Ces deux mécanismes sont décrits dans cette Recommandation.

Le mécanisme de découverte vise à trouver les sept types d'informations sur la cybersécurité suivants: base de données sur les ressources de l'utilisateur, base de données sur les ressources du fournisseur, base de données sur les incidents, base de données sur les avertissements, base de connaissances sur les produits et services, base de connaissances sur les cyberrisques et base de connaissances sur les contre-mesures. L'acquisition, le regroupement et l'utilisation des informations sur la cybersécurité, qui comprennent un ensemble de domaines d'opérations, de rôles et de types d'informations, sont décrites sous la forme du modèle présenté dans la Figure 41, laquelle montre en outre le lien entre les types d'information utilisés dans ce modèle.



BD: Base de données
BC: Base de connaissances

Figure 41 – Ontologie des informations opérationnelles de cybersécurité

Les rôles, représentés sous forme d'icônes humaines sur la figure, sont génériques et des entités comme les CIRT peuvent englober une ou plusieurs de ces fonctions. On utilise ce modèle pour définir des domaines d'opérations de cybersécurité, lesquels servent ensuite à identifier les entités de cybersécurité requises pour prendre en charge les opérations dans chaque domaine.

9.2 Prise en charge des incidents

Procéder de manière cohérente à la détection des incidents de sécurité, à leur traitement et à la diffusion d'informations à leur sujet fait partie des activités courantes liées à la gestion de la sécurité. En l'absence d'une évaluation et d'une prise en charge adaptées de ce type d'incidents, les organisations s'exposeront à d'autres attaques risquant d'être plus graves.

Faute d'une procédure de prise en charge des incidents, en cas de détection d'un incident lié à la sécurité, il se peut que cet incident ne soit pas notifié ou analysé correctement. Il se peut aussi qu'il n'existe pas de procédures pour faire remonter cette notification ou obtenir une assistance technique ou des orientations auprès des responsables, alors même que les problèmes que pose ce type d'incident ont souvent des conséquences bien au-delà des technologies de l'information ou des réseaux. Par exemple, un incident peut avoir des conséquences sur le plan juridique ou financier, sur la réputation de l'entreprise ou d'un point de vue de l'application de la loi. Sans procédure de prise en charge efficace des incidents, on risque d'avoir recours à une solution "bricolée" ou provisoire, au lieu de traiter, de décrire et de notifier correctement le problème, d'où le risque de s'exposer à un problème plus grave par la suite.

A mesure que les organisations prennent conscience de la nécessité de gérer de manière cohérente et efficace la sécurité des réseaux et de leur exploitation, la prise en charge des incidents devient une tâche plus régulière. Un personnel correctement formé avec des attributions bien définies peut traiter rapidement et de manière adéquate les incidents liés à la sécurité.

Pour parvenir à prendre en charge les incidents et à les notifier, il faut comprendre comment ils sont détectés, gérés et résolus. L'établissement d'une structure de traitement des incidents (à savoir, les incidents physiques, administratifs ou organisationnels et logiques) permet d'obtenir une image de la structure et du déroulement d'un incident. La *Recommandation UIT-T E.409* donne des orientations permettant de préparer une organisation à détecter et traiter des incidents liés à la sécurité. Elle est générique par nature et n'a pas pour vocation à définir ou aborder des exigences pour des réseaux particuliers.

Il est essentiel d'utiliser de manière cohérente la terminologie lors de la notification ou de la prise en charge d'un incident. L'emploi d'une terminologie différente peut entraîner une mauvaise compréhension, le risque étant par la suite qu'un incident lié à la sécurité ne soit pas pris au sérieux ou traité rapidement en vue de limiter ses effets ou d'empêcher qu'il se reproduise. En outre, la définition de ce que l'on considère comme un incident peut varier suivant les professions, les organisations et les personnes. La Recommandation UIT-T E.409 définit la terminologie concernant la détection et la notification des incidents, et montre comment classer les incidents en fonction de leur gravité (voir la Figure 42).

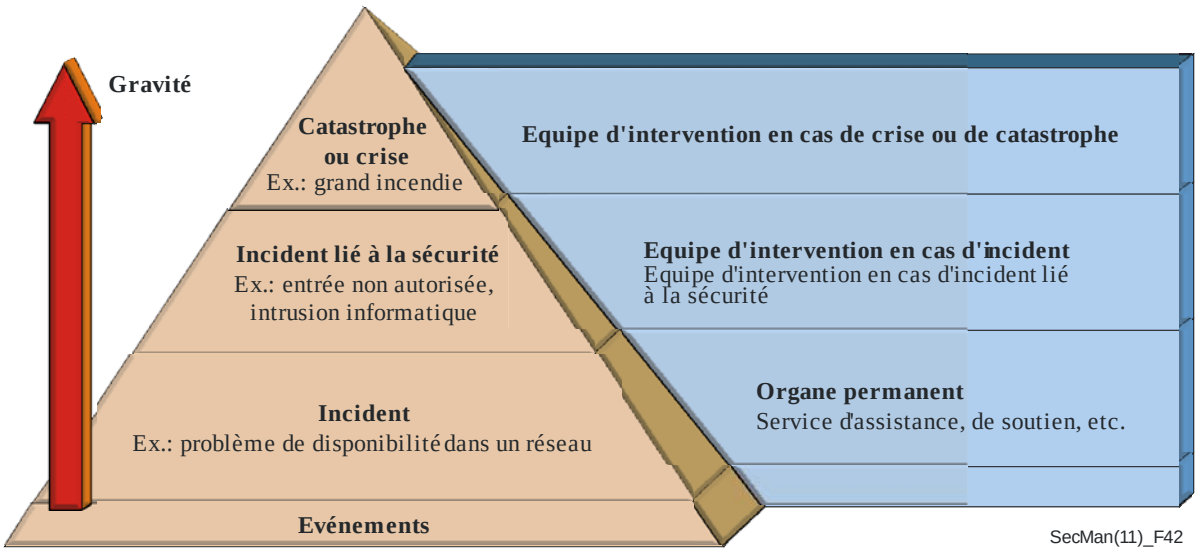


Figure 42 – Pyramide des événements et des incidents décrite dans la Recommandation UIT-T E.409

La Recommandation UIT-T E.409 définit en outre une structure de prise en charge des incidents (voir la Figure 43) et décrit des procédures permettant de détecter, de classer, d'évaluer, de traiter et de suivre les incidents.

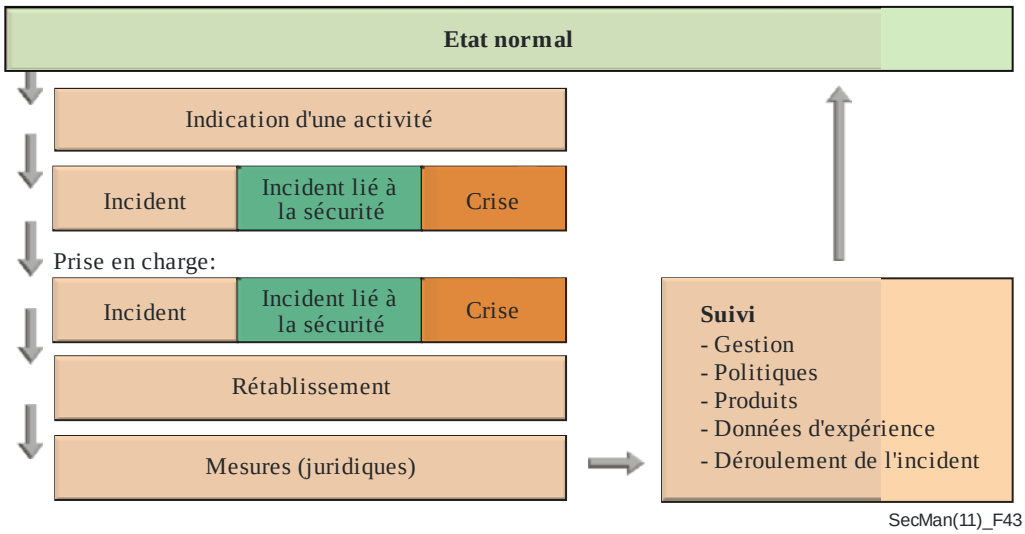


Figure 43 – Structure de la prise en charge d'un incident décrite dans la Recommandation UIT-T E.409

La Recommandation UIT-T X.1056 approuvée il y a peu s'appuie sur les orientations données dans la Recommandation UIT-T E.409. Les organisations de télécommunication doivent avoir des procédures leur permettant à la fois de prendre en charge les incidents et de les empêcher de se reproduire. Cinq procédures de gestion des incidents de haut niveau – préparation, protection, détection, tri et réponse – sont décrites dans la Recommandation UIT-T X.1056, ainsi que le lien avec la gestion de la sécurité. Ces procédures font l'objet de la Figure 44.

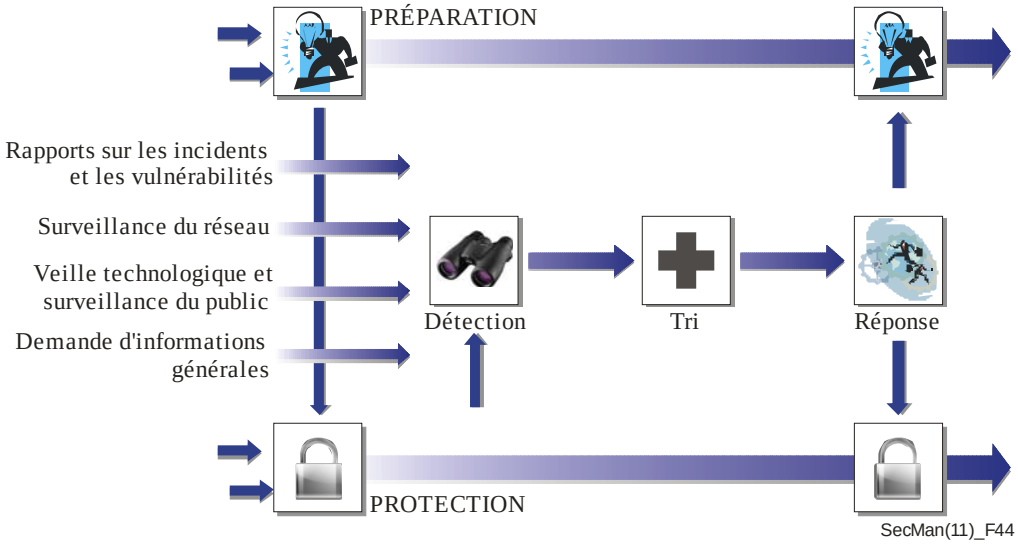


Figure 44 – Cinq procédures de gestion des incidents de haut niveau

En outre, la Recommandation UIT-T X.1056 dresse une liste de services proactifs, de services réactifs et de services de gestion de la qualité de la sécurité qu'une équipe de gestion des incidents de sécurité peut assurer.

10. Sécurité des applications

10 Sécurité des applications

De plus en plus conscients de l'importance de la sécurité, les développeurs d'application font aujourd'hui davantage attention à la nécessité d'intégrer la sécurité dans leurs produits, plutôt que d'essayer de mettre en œuvre la sécurité après coup au stade de la production. Malgré cela, certaines vulnérabilités intrinsèques sont découvertes dans la plupart des applications, à un moment ou à un autre de leur cycle de vie. De plus, l'évolution des menaces a souvent pour effet d'exposer des vulnérabilités auparavant inconnues qui sont alors exploitées.

Dans ce chapitre, on examine les fonctionnalités de sécurité d'un certain nombre d'applications des TIC, en mettant l'accent sur les fonctionnalités de sécurité définies dans les Recommandations UIT-T.

10.1 Téléphonie IP (VoIP) et multimédia

La téléphonie IP, également appelée voix sur IP (VoIP, *voice-over-IP*), désigne la fourniture de services traditionnellement offerts par le réseau téléphonique public commuté (RTPC) à commutation de circuit via un réseau utilisant le protocole Internet (IP). Parmi ces services figurent essentiellement les communications téléphoniques, mais aussi d'autres formes de média, y compris la vidéo et les données. La téléphonie IP inclut aussi de nombreux autres services complémentaires associés et services de réseau intelligent tels que les conférences (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". La téléphonie sur Internet est un cas particulier de déploiement de la VoIP, dans lequel le trafic téléphonique est acheminé sur le réseau dorsal Internet public.

La Recommandation UIT-T H.323 est une Recommandation cadre qui jette les bases des communications audio, vidéo et de données sur les réseaux à commutation par paquets, y compris l'Internet, les réseaux locaux (LAN, *local-area network*) et les réseaux étendus (WAN, *wide-area network*), 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 paquets et échange de paquets Internet (IPX) sur Ethernet, Fast Ethernet et Token Ring. Les produits et applications multimédias issus de différents fabricants mais conformes à la Recommandation UIT-T H.323 peuvent interfonctionner, ce qui permet aux utilisateurs de communiquer sans avoir à se soucier de la compatibilité. La Recommandation UIT-T H.323 a défini le premier protocole de téléphonie IP et elle est considérée comme la pierre angulaire pour les produits fondés sur la téléphonie IP destinés aux particuliers, aux entreprises, aux fournisseurs de services et au secteur du divertissement. Les spécifications de sécurité pour les Recommandations UIT-T de la série H.323 sont énoncées dans le *Guide de mise en oeuvre de la Recommandation UIT-T H.235 V3*, dans les Recommandations UIT-T de la série H.235.x, qui comprend neuf cadres et normes de sécurité, et dans la Recommandation UIT-T H.530. La mobilité pour systèmes et services multimédias UIT-T H.323 fait l'objet de la Recommandation UIT-T H.510.

La Recommandation UIT-T H.323, au domaine d'application vaste, porte à la fois sur la mise en oeuvre de dispositifs autonomes et sur une intégration de la technologie dans les ordinateurs personnels ainsi que sur les communications point à point et multipoint.

La Recommandation UIT-T H.323 définit quatre principaux composants pour un système de communication fondé sur le réseau: terminaux, passerelles, portiers et unités de commande multipoint. En outre, des éléments frontières ou homologues sont également possibles. Ces éléments apparaissent sur la Figure 45.

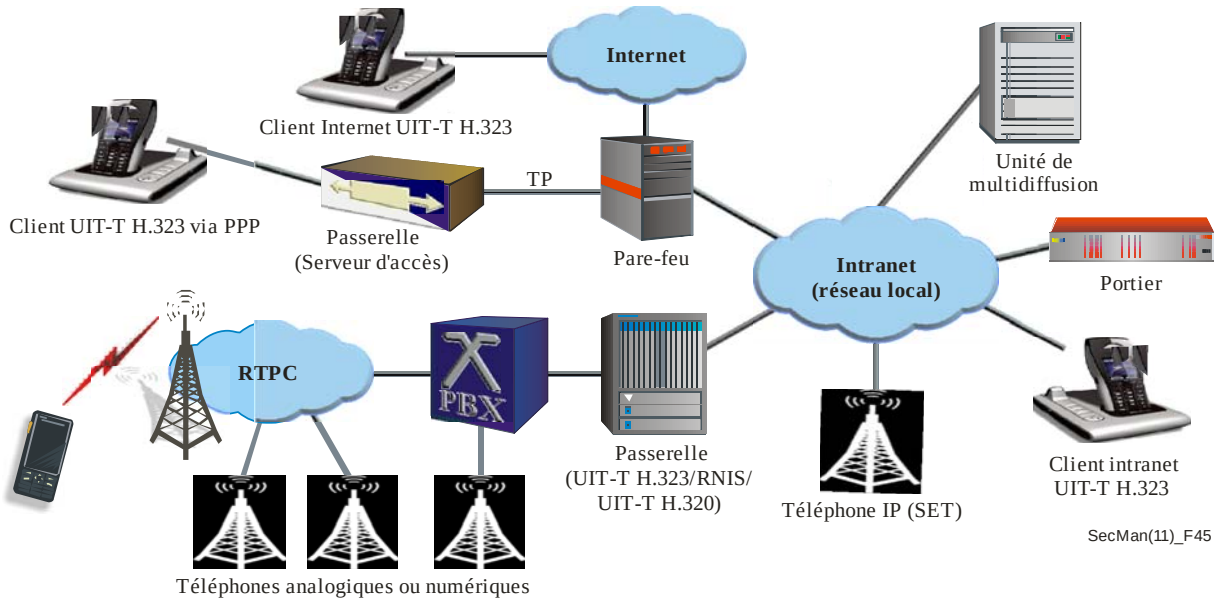


Figure 45 – Système UIT-T H.323: composants et scénarios de déploiement

La Recommandation UIT-T H.323 est par exemple utilisée pour le transit en masse par les opérateurs, notamment dans les réseaux dorsaux de téléphonie IP et pour les services de carte d'appel. Dans les entreprises, elle est utilisée pour les autocommutateurs IP, les centrex IP, les réseaux privés virtuels téléphoniques, les systèmes de téléphonie et de données intégrés, les téléphones Wi-Fi, la mise en oeuvre de centres d'appel et les services de mobilité. Elle est largement utilisée pour les conférences téléphoniques et les visioconférences, la collaboration téléphonie/données/vidéo et l'enseignement à distance. Les particuliers l'emploient notamment pour l'accès audiovisuel à large bande et pour les communications de PC à téléphone, de téléphone à PC ou de PC à PC.

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

Tous les éléments d'un système UIT-T H.323 peuvent être répartis géographiquement et, les réseaux IP étant ouverts, il existe plusieurs menaces de sécurité, comme l'illustre la Figure 46.

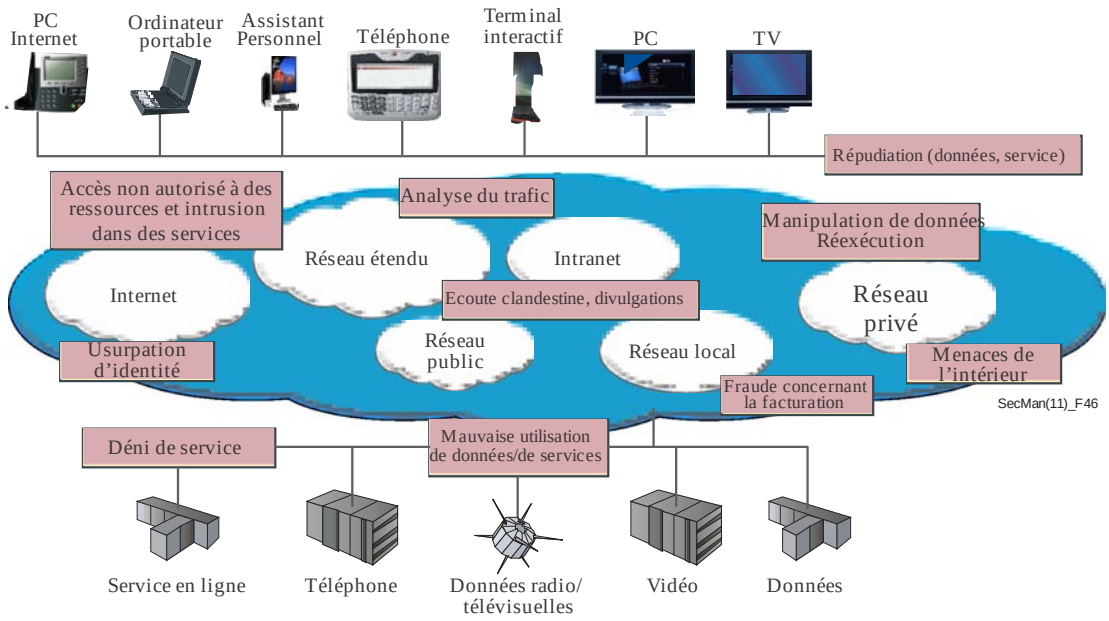


Figure 46 – Menaces de sécurité dans les communications multimédias

Les principales exigences de sécurité pour les communications multimédias et la téléphonie IP sont les suivantes:

- 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. Condition indispensable à l'authentification, l'utilisateur et/ou le terminal doit être identifié. Il doit ensuite 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 UIT-T X.509).

- Authentification de serveur: Etant donné que les utilisateurs de téléphonie IP communiquent généralement entre eux grâce à une infrastructure de téléphonie IP faisant intervenir des serveurs, des passerelles et, éventuellement, des techniques de multidiffusion, les utilisateurs fixes comme les utilisateurs mobiles ont besoin de savoir s'ils sont reliés au serveur correct et/ou au fournisseur de services correct.

- Authentification d'utilisateur/de terminal et de serveur: Elle est nécessaire pour lutter contre les menaces de sécurité, telles que l'usurpation d'identité, les attaques de l'intercepteur, l'usurpation d'adresse IP et le détournement de connexion.

- Autorisation d'appel: Il s'agit du processus qui consiste à déterminer si l'utilisateur/le terminal est réellement autorisé à utiliser une fonctionnalité de service (appel dans le RTPC, etc.) ou une ressource de réseau. Le plus souvent, les fonctions d'authentification et d'autorisation sont utilisées ensemble pour prendre une décision au niveau du contrôle d'accès. L'authentification et l'autorisation aident à contrecarrer les attaques de type usurpation d'identité, utilisation abusive et fraude, manipulation et déni de service.

- Protection de sécurité de la signalisation: Il s'agit de protéger les protocoles de signalisation contre les manipulations et les utilisations abusives et d'assurer la confidentialité et le respect de la vie privée. Pour protéger les protocoles de signalisation, on utilise généralement le chiffrement et des mesures de protection de l'intégrité et de protection contre les réexécutions. Il faut tout particulièrement veiller à ce que les exigences essentielles de qualité de fonctionnement pour les communications en temps réel soient respectés afin d'éviter toute dégradation de service due au traitement de la sécurité.

- Confidentialité des signaux vocaux et des médias: Cette confidentialité est obtenue grâce au chiffrement des paquets téléphoniques (protection contre les écoutes clandestines) et des paquets de média (par exemple vidéo) des applications multimédias. La protection renforcée des paquets de média comprend également l'authentification/la protection de l'intégrité des données utiles.

- Gestion de clés: La gestion de clés peut être exécutée en dehors de l'application de téléphonie IP (configuration 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.

- Sécurité interdomaines: Elle prend en compte le problème qui se pose lorsque 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 particulièrement important lorsque des frontières entre domaines sont franchies et lorsque 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 traducteurs d'adresse de réseau (NAT, *network address translation*).

Cette liste n'est pas exhaustive, mais il s'agit là des aspects essentiels liés à la sécurité abordés dans la Recommandation UIT-T H.323. Parmi les aspects liés à la sécurité qui sont considérés comme ne faisant pas partie du domaine d'application de la Recommandation UIT-T H.323, on peut citer la politique de sécurité, la sécurité de gestion de réseau, la configuration de la sécurité, la sécurité de mise en œuvre, la sécurité opérationnelle et la prise en charge des incidents de sécurité. La Recommandation UIT-T X.1101 contient les exigences de sécurité pour les communications en multidiffusion.

10.1.2 Aperçu des Recommandations UIT-T de la sous-série H.235.x

Les Recommandations UIT-T de la série H.235.x comprennent onze normes et un guide de mise en œuvre qui, ensemble, spécifient les mécanismes et protocoles de sécurité et donnent des indications détaillées sur la mise en œuvre de la sécurité dans le cadre des Recommandations UIT-T de la série H.323. Elles décrivent des solutions de sécurité modulables pour des petits groupes, des entreprises et des exploitants de grande envergure et permettent d'assurer la protection cryptographique des protocoles de commande et des données de flux médias audio/vidéo.

Les Recommandations UIT-T de la série H.235 présentent des moyens permettant de négocier les services cryptographiques, les algorithmes de chiffrement et les capacités de sécurité 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. Les configurations prises en charge comprennent la configuration point à point "classique" et les configurations multipoint avec unités de multidiffusion dans lesquelles plusieurs terminaux multimédias communiquent au sein d'un groupe.

Les Recommandations UIT-T de la série H.235 utilisent des techniques de sécurité optimisées particulières (cryptographie à courbe elliptique et chiffrement AES par exemple) afin de respecter les contraintes strictes de qualité de fonctionnement. Lorsque le chiffrement téléphonique est mis en œuvre, on procède au

chiffrement des données utiles RTP dans la couche application. Cette façon de procéder a peu d'incidence sur les points d'extrémité grâce à une interaction étroite avec le processeur de signaux numériques et les codecs de compression vocale et ne dépend pas d'une plate-forme de système d'exploitation particulière.

La Figure 47 illustre le domaine d'application des Recommandations UIT-T de la série H.235, qui contiennent des dispositions relatives à l'établissement d'appels (blocs UIT-T H.225.0 et UIT-T H.245) et de communications bidirectionnelles (chiffrement de données utiles RTP contenant des signaux audio et/ou vidéo compressés) et prévoient des mécanismes de sécurité pour l'authentification, l'intégrité, le respect de la vie privée et la non-répudiation. Les portiers sont chargés d'assurer l'authentification en procédant à un contrôle de l'admission au niveau des points d'extrémité et de fournir des mécanismes de non-répudiation. La sécurité dans la couche de transport et dans les couches inférieures, fondées sur IP, sort du cadre de la Recommandation UIT-T H.323 et des Recommandations UIT-T de la série H.235, mais elle est couramment mise en œuvre au moyen des protocoles de sécurité IP (IPSec) et de sécurité dans la couche transport (TLS, *transport layer security*). Lorsque la politique du système d'extrémité l'exige, le protocole IPSec ou TLS peut être utilisé pour assurer l'authentification et, facultativement, la confidentialité dans la couche IP quel que soit le protocole (d'application) qui est exécuté au-dessus.

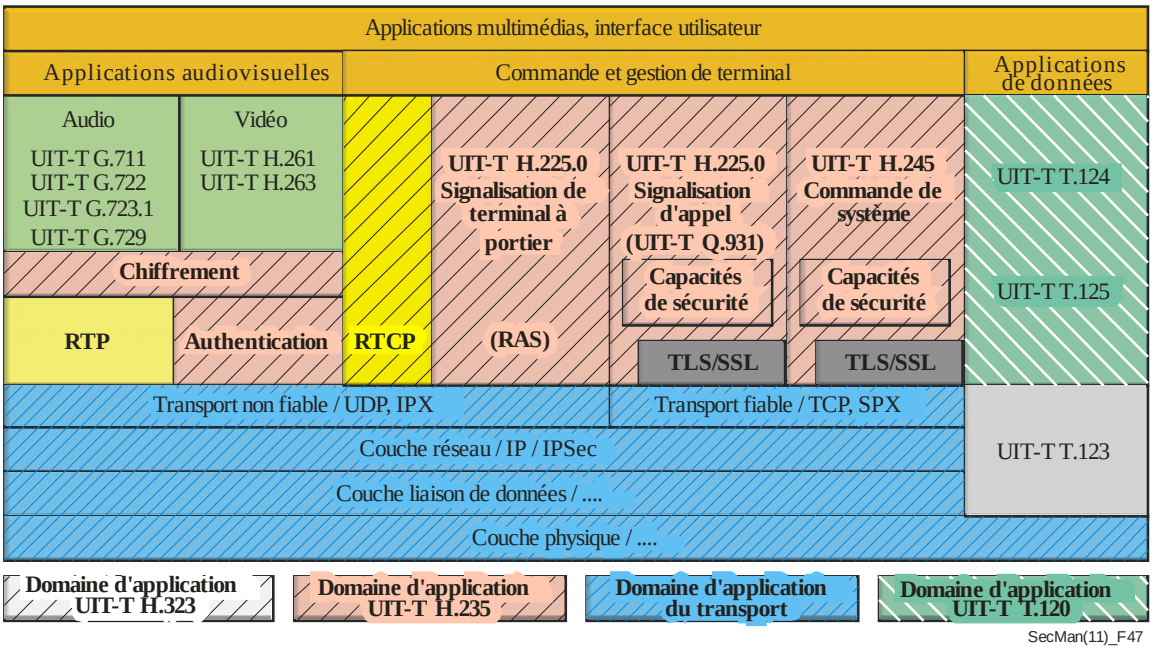


Figure 47 – Sécurité des systèmes UIT-T H.323 définie dans les Recommandations UIT-T de la série H.235

Les Recommandations UIT-T de la série UIT-T H.235.x décrivent une large palette de mesures de sécurité qui sont applicables dans différents environnements cibles (par exemple les environnements intra/inter-entreprises et les environnements d'opérateurs) et qui peuvent être adaptées aux besoins et propres à un scénario, en fonction de facteurs locaux tels que l'infrastructure de sécurité disponible et les capacités de terminal (par exemple points d'extrémité simples ou points d'extrémité intelligents).

Les profils de sécurité disponibles vont de simples profils à secret partagé avec mot de passe protégé à des profils plus complexes avec signatures numériques et certificats PKI de la Recommandation UIT-T X.509 (Recommandation UIT-T H.235.2). 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. La Recommandation UIT-T H.235.3 est appelée profil de sécurité hybride car elle combine les procédures de sécurité symétriques de la Recommandation UIT-T H.235.1 avec les signatures et certificats fondés sur l'infrastructure PKI et les signatures de la Recommandation UIT-T H.235.2, ce qui permet d'optimiser la qualité de fonctionnement et de raccourcir les temps d'établissement

d'appel. La Recommandation UIT-T H.235.4 définit des mesures de sécurité visant à sécuriser un modèle d'homologue à homologue. Elle définit en outre des procédures de gestion de clés dans des environnements d'entreprise et dans des environnements interdomaines.

Afin d'assurer une plus grande sécurité des systèmes qui utilisent des numéros d'identification personnels (PIN, *personal identification number*) ou des mots de passe pour authentifier les utilisateurs, la Recommandation UIT-T H.235.5 définit un autre "*cadre de l'authentification sécurisée pendant l'échange de messages RAS au moyen de secrets partagés faibles*" fondé sur l'utilisation de méthodes à clé publique pour sécuriser l'utilisation des numéros PIN/mots de passe. La Recommandation UIT-T H.235.6 rassemble toutes les procédures qui sont nécessaires pour le chiffrement du flux de médias RTP, y compris la gestion de clés associée.

La mobilité des utilisateurs et des terminaux en toute sécurité dans des environnements UIT-T H.323 répartis fait l'objet de la Recommandation UIT-T H.530, qui aborde 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; et
- protection des données de signalisation entre un terminal mobile et un domaine visité.

La Recommandation UIT-T H.235.0 décrit le cadre général de sécurité pour les systèmes multimédias de la série H. La Recommandation UIT-T H.235.0 et les Recommandations UIT-T de la série H.350 définissent une gestion de clés modulable fondée sur le protocole rapide d'accès à l'annuaire (LDAP, *lightweight directory access protocol*) et la couche de connecteurs sécurisés (SSL/TLS, *secure socket layer*). En particulier, les Recommandations UIT-T de la série H.350 définissent des capacités qui permettent aux entreprises et aux opérateurs de gérer en toute sécurité de très nombreux utilisateurs de services de vidéo et téléphonie IP et permet de relier les systèmes UIT-T H.323, SIP, UIT-T 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.

10.1.3 Traducteurs d'adresse de réseau et pare-feu

L'Internet a été conçu suivant le principe "de bout en bout". Autrement dit, deux dispositifs quelconques raccordés au réseau peuvent communiquer directement entre eux. Toutefois, en raison de préoccupations liées à la sécurité et d'un manque d'adresses de réseau IPv4, des pare-feu (FW) et des traducteurs d'adresse de réseau (NAT) sont souvent employés à la frontière des réseaux. Ces frontières entourent le domaine résidentiel, le domaine du fournisseur de services, le domaine de l'entreprise et quelquefois le domaine du pays. Parfois, plusieurs pare-feu ou dispositifs NAT sont employés dans un même domaine. Les pare-feu sont conçus pour contrôler le passage des informations à travers les frontières de réseau et sont généralement configurés pour bloquer la plupart des communications IP. Si un pare-feu n'est pas configuré explicitement pour laisser passer le trafic UIT-T H.323 provenant de dispositifs externes afin que ce trafic aboutisse aux dispositifs UIT-T H.323 internes, la communication est tout simplement impossible, ce qui pose problème pour tout utilisateur d'équipement UIT-T H.323.

Les traducteurs NAT traduisent les adresses utilisées dans le domaine interne en adresses utilisées dans le domaine externe et inversement. Les adresses utilisées dans un domaine résidentiel ou dans un domaine d'entreprise sont généralement, mais pas toujours, attribuées à partir des espaces d'adresses de réseau privé définis dans la norme IETF RFC 1918, qui sont les suivants:

Classe	Intervalle d'adresses	Nombre d'adresses IP
A	10.0.0.0 – 10.255.255.255	16 777 215
B	172.16.0.0 – 172.31.255.255	1 048 575
C	192.168.0.0 – 192.168.255.255	65 535

Les dispositifs NAT posent un problème encore plus compliqué pour la plupart des protocoles IP, en particulier ceux qui acheminent des adresses IP dans le protocole. Les protocoles UIT-T H.323, SIP et d'autres protocoles de communication en temps réel qui fonctionnent sur des réseaux à commutation par paquets doivent fournir des informations de port et d'adresse IP de sorte que les autres participants à la communication sachent où envoyer les flux de média (par exemple flux audio et vidéo).

Les questions relatives à la traversée des dispositifs NAT/FW sont abordées dans trois Recommandations UIT-T de la série H.460, qui permettent aux communications UIT-T H.323 de traverser de façon transparente un ou plusieurs dispositifs NAT/FW. Il s'agit des Recommandations UIT-T H.460.17, UIT-T H.460.18 et UIT-T H.460.19.

La Figure 48 montre comment un "proxy" spécial pourrait être utilisé pour permettre aux flux provenant de dispositifs "non compatibles" NAT/FW de traverser facilement et correctement les dispositifs NAT/FW.

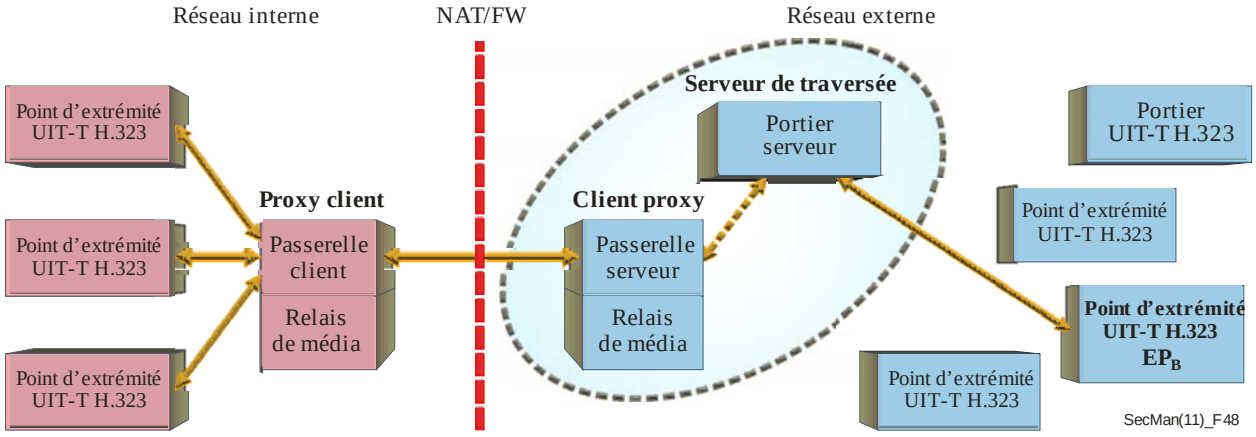


Figure 48 – Traversée de dispositifs NAT/FW dans l'architecture UIT-T H.460.18

La topologie ci-dessus peut par exemple être utilisée lorsqu'une entreprise souhaite contrôler la route que les flux de signalisation d'appel et de média UIT-T H.323 empruntent dans le réseau. Toutefois, les Recommandations UIT-T H.460.17 et UIT-T H.460.18 permettent aussi aux flux provenant de points d'extrémité de traverser les dispositifs NAT/FW sans l'aide d'un "proxy" interne spécial. La Figure 49 illustre la topologie correspondante.

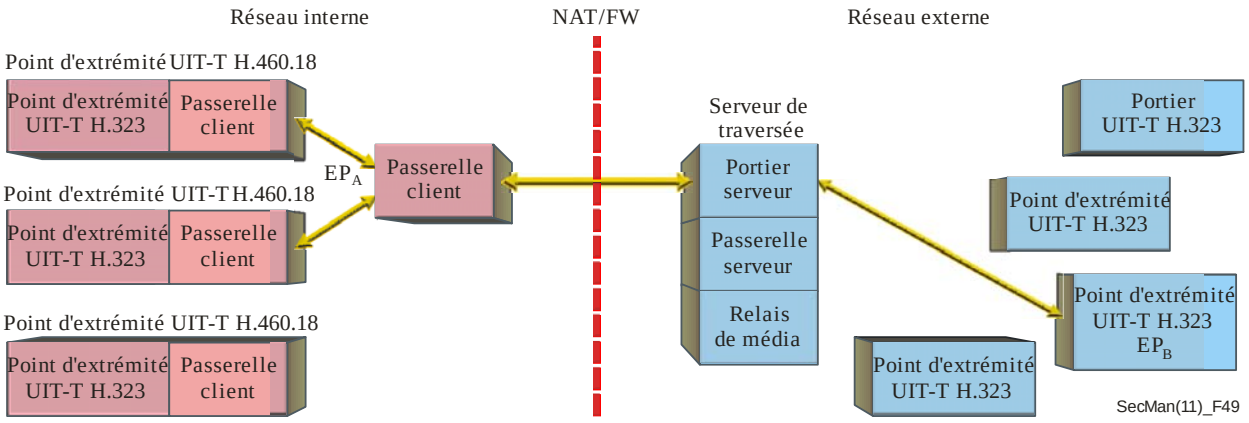


Figure 49 – Architecture avec communication entre portiers

Sur la Figure 49, les points d'extrémité du réseau interne communiquent avec le portier du réseau interne pour résoudre l'adresse des entités externes (par exemple, une adresse IP obtenue à partir d'un numéro de téléphone ou d'une adresse URL UIT-T H.323). Le portier du réseau interne communique avec un portier du réseau externe pour échanger ces informations d'adressage et achemine ces informations au point d'extrémité appelant. Lorsqu'un dispositif situé dans le réseau interne lance un appel à destination d'un dispositif situé dans le réseau externe, il utilisera les procédures définies dans la Recommandation UIT-T H.460.18 pour ouvrir les "microtrous" nécessaires dans les dispositifs NAT/FW pour laisser passer la signalisation du réseau interne au réseau externe. Il utilisera en outre les procédures définies dans la Recommandation UIT-T H.460.19 pour ouvrir les "microtrous" nécessaires pour permettre aux flux de médias de passer correctement du réseau interne au réseau externe et inversement.

Lorsque les dispositifs appelant et appelé sont situés dans des réseaux privés différents séparés par des dispositifs NAT/FW et l'Internet public, au moins une "passerelle serveur" et un "relais de média" (définis dans la Recommandation UIT-T H.460.18) sont nécessaires pour pouvoir acheminer correctement la signalisation et les médias entre les deux réseaux privés. Cette combinaison de dispositifs est généralement appelée "contrôleur de limite de session". La raison en est simple: par conception, un paquet IP provenant d'un réseau privé ne peut pénétrer dans un autre réseau privé qu'avec l'aide d'une entité ("proxy") du réseau public.

10.2 TVIP

Les dispositions prises pour la sécurité de la télévision par protocole Internet (TVIP) doivent permettre de protéger les contenus acheminés par le biais des services de TVIP, les dispositifs terminaux utilisés et la fourniture de ces services.

La protection de contenu de TVIP consiste à faire en sorte qu'un utilisateur final ne puisse utiliser le contenu qu'en fonction des droits que lui a octroyés le titulaire des droits. Il s'agit notamment de protéger les contenus contre la copie et la distribution illégales, l'interception, la falsification et l'utilisation non autorisée.

La protection des dispositifs terminaux de TVIP consiste à faire en sorte que le dispositif dont se sert un utilisateur final pour recevoir un service puisse utiliser en toute sécurité et fiabilité le contenu, les droits d'utilisation du contenu étant respectés et l'intégrité et la confidentialité du contenu et des paramètres de sécurité essentiels tels que les clés de chiffrement étant protégées.

La protection des services de TVIP consiste à faire en sorte que les utilisateurs finals ne puissent acquérir que le service et le contenu qu'ils sont habilités à recevoir. Il s'agit notamment de protéger le service contre tout accès non autorisé.

Plusieurs Recommandations portant spécifiquement sur la sécurité de la TVIP ont été approuvées. La Recommandation UIT-T X.1191 définit l'architecture générale de sécurité de la TVIP (voir la Figure 50). Il est à noter que seules les fonctions qui s'appliquent à l'utilisateur final, au fournisseur de réseau et au fournisseur de services sont considérées comme faisant partie du domaine d'application de la Recommandation. Les fonctions se rapportant au fournisseur de contenu font l'objet d'accords privés entre les parties prenantes et sont considérées comme ne faisant pas partie du domaine d'application de cette Recommandation.

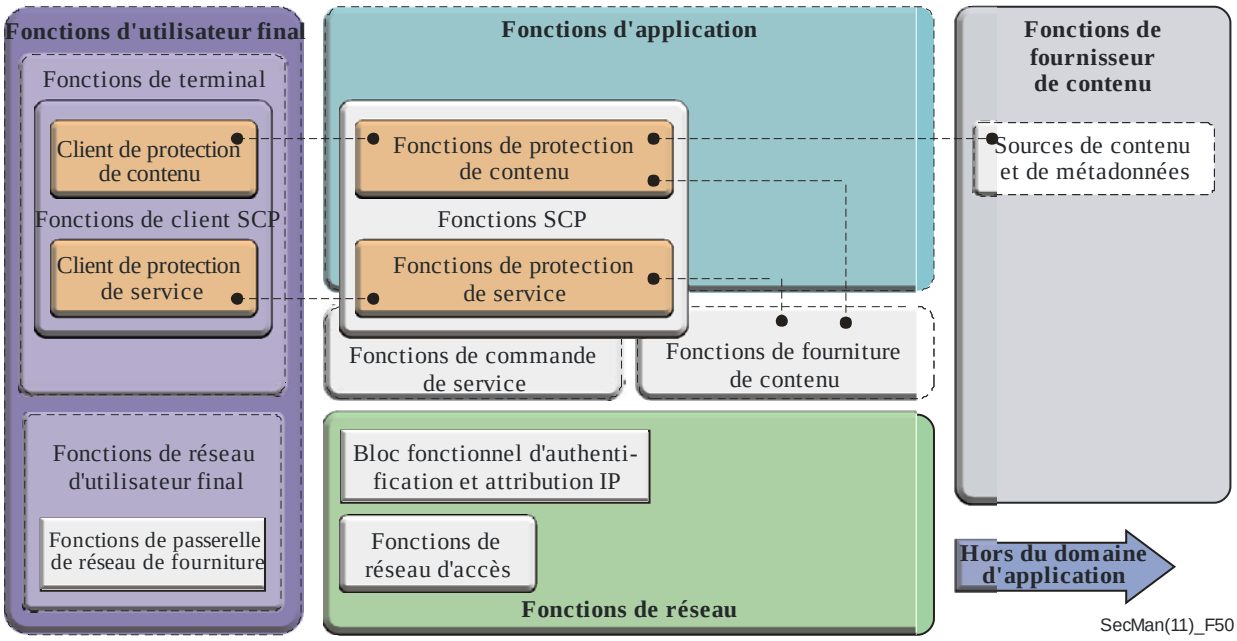


Figure 50 – Architecture générale de sécurité pour la TVIP

10.2.1 Mécanismes de protection de contenu de TVIP

Les mécanismes de sécurité qui peuvent être utilisés pour protéger un contenu sont notamment les suivants:

- chiffrement du contenu;
- filigranage (par exemple l'utilisation de la stéganographie pour modifier certaines caractéristiques du contenu sans que cette modification puisse être détectée facilement);
- identification et informations de traçage de contenu afin de faciliter les investigations en cas d'accès non autorisé à un contenu ou d'utilisation non autorisée d'un contenu;
- étiquetage du contenu (par exemple avec des informations de notation pour permettre aux utilisateurs finals d'avoir un certain contrôle sur l'accès à un contenu approprié); et
- transcodage sécurisé (qui permet aux nœuds de réseau intermédiaires de changer le format ou la qualité d'un contenu multimédia sans déchiffrement, d'où une préservation de la sécurité de bout en bout).

10.2.2 Mécanismes de protection des services de TVIP

Les mécanismes de protection des services sont notamment les suivants:

- authentification de l'utilisateur final (abonné) et/ou du dispositif terminal;
- autorisation (pour s'assurer que l'utilisateur final ou le terminal est autorisé à accéder aux services et/ou au contenu); et
- contrôle d'accès (tout particulièrement pour faire en sorte que seul un fournisseur de services autorisé puisse accéder au contenu qui est téléchargé d'un client vers un serveur).

La Recommandation UIT-T X.1192 définit des exigences fonctionnelles et des mécanismes relatifs au transcodage sécurisé pour la TVIP, la Recommandation UIT-T X.1193 contient un cadre de gestion des clés pour les services sécurisés de télévision utilisant le protocole Internet (TVIP) et la Recommandation UIT-T X.1195 présente un mécanisme d'interopérabilité de la protection de service et de contenu (SCP).

10.2.3 Protection des informations d'abonné

Lors de la mise en œuvre de la TVIP, il faut bien prendre en compte la nécessité de protéger les informations d'abonné qui peuvent inclure des données qui sont suivies comme le numéro de chaîne avant et après un changement de chaîne, l'heure du changement, des informations d'utilisateur pour le service de guide de programmes électronique, l'identification du paquetage, l'heure de lecture, etc. Ces données doivent être considérées comme sensibles et des mesures doivent être prises pour éviter toute divulgation non autorisée via le terminal, le réseau ou le fournisseur de services. Des suggestions pour protéger les informations d'abonné sont formulées dans une annexe à la Recommandation UIT-T X.1191.

10.3 Transmission de télécopie sécurisée

La télécopie reste une application courante, mais la confiance dans les services de télécopie dépend fortement de l'efficacité des mesures de sécurité intégrées. Au départ, les normes de télécopie ont été élaborées pour une transmission sur le RTPC (Recommandation UIT-T T.4), puis pour une transmission sur le RNIS (Recommandation UIT-T T.563). Plus récemment, des extensions ont été spécifiées pour la transmission de télécopie en temps réel sur les réseaux IP (y compris l'Internet) (Recommandation UIT-T T.38) et via des systèmes avec stockage et retransmission (Recommandation UIT-T T.37).

Quel que soit le mode de transmission, les problèmes de sécurité affectant les services de télécopie concernent la confidentialité des données transmises, l'authentification et la non-répudiation. Ces problèmes sont devenus d'autant plus importants que le trafic s'est déplacé sur l'Internet, en raison du caractère ouvert et réparti du support.

La sécurité de la transmission de télécopie fait l'objet de la Recommandation UIT-T T.36, qui définit deux solutions techniques indépendantes pouvant être utilisées pour le chiffrement des documents échangés. L'une des solutions consiste à utiliser l'algorithme de chiffrement de *Rivest, Shamir & Adleman* (RSA), tandis que l'autre consiste à utiliser une combinaison de *Hawthorne Key Management* (HKM) et de *Hawthorne Facsimile Cipher* (HFX). Les services de sécurité définis sont les suivants:

- authentification mutuelle (obligatoire);
- service de sécurité (facultatif) incluant l'authentification mutuelle, l'intégrité des messages et la confirmation de réception des messages;

- service de sécurité (facultatif) incluant l'authentification mutuelle, la confidentialité des messages (chiffrement) et l'établissement de clé de session; et

- service de sécurité (facultatif) incluant l'authentification mutuelle, l'intégrité des messages, la confirmation de réception des messages, la confidentialité des messages (chiffrement) et l'établissement de clé de session.

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

- authentification d'entité mutuelle;

- établissement de clé de session secrète;

- confidentialité de document;

- confirmation de réception; et

- confirmation ou réfutation d'intégrité de document.

10.4 Services web

Les technologies web, en particulier les architectures orientées service (SOA, *service-oriented architecture*), sont largement utilisées car elles permettent de développer et de déployer de nouveaux services de façon efficace et peu onéreuse, et d'intégrer des contenus provenant de diverses sources pour former des services composites facilement et rapidement. Les aspects de sécurité des services web sont nombreux. Il faut prévoir des mécanismes d'authentification et de connexion unique (SSO, *single sign-on*) ainsi que des mécanismes de sécurité pour prendre en charge les services web mobiles.

Les économies d'échelle ont conduit les fabricants de plates-formes informatiques à développer des produits ayant des fonctionnalités très générales, de sorte qu'ils puissent être utilisés dans la plus large gamme possible de situations. Ces produits sont fournis avec le plus de privilèges possible concernant l'accès aux données et l'exécution des logiciels, afin qu'ils puissent être utilisés dans le plus grand nombre possible d'environnements d'application, y compris ceux qui ont les politiques de sécurité les plus permissives. Lorsqu'une politique de sécurité plus restrictive est requise, les privilèges intrinsèques de la plate-forme doivent être restreints par une configuration locale.

La politique de sécurité d'une grande entreprise comporte de nombreux éléments et de nombreux points d'application. Les éléments de la politique peuvent être gérés par différents services de l'organisation (systèmes d'information, sécurité, ressources humaines, affaires juridiques, etc.) et depuis différents points d'application (extranet, réseau étendu ou systèmes d'accès à distance). Il est courant que chaque point d'application soit géré de façon indépendante.

L'utilisation d'un langage commun pour exprimer la politique de sécurité permet à l'entreprise de gérer l'application de tous les éléments de sa politique de sécurité dans tous les composants de ses systèmes d'information. La gestion de la politique de sécurité peut inclure tout ou partie des étapes suivantes: rédaction, révision, test, approbation, publication, combinaison, analyse, modification, retrait, consultation et application de la politique.

En outre, un cadre est nécessaire pour les échanges d'informations de sécurité. Pour faciliter ces échanges, des langages de balisage ont été élaborés, dont le langage de balisage d'assertion de sécurité et le langage de balisage extensible de contrôle d'accès (XACML, *eXtensible Access Control Markup Language*). Elaborés au départ par OASIS, ces langages ont ensuite été adoptés et publiés par l'UIT-T avec l'assistance d'OASIS.

10.4.1 Langage de balisage d'assertion de sécurité

La Recommandation UIT-T X.1141 définit le langage de balisage d'assertion de sécurité (SAML 2.0), qui est un cadre fondé sur XML pour l'échange d'informations de sécurité. Ces informations de sécurité sont exprimées sous la forme d'*assertions* sur des *sujets*, où un sujet est une entité qui a une identité dans un certain domaine de sécurité. Une même assertion peut contenir plusieurs déclarations internes différentes concernant l'authentification, l'autorisation et les attributs.

En principe, un certain nombre de *fournisseurs de services* peuvent utiliser des assertions sur un sujet afin de contrôler l'accès et fournir un service personnalisé et, en conséquence, ils deviennent la partie utilisatrice d'une partie assertante appelée *fournisseur d'identité*.

La Recommandation UIT-T X.1141 définit trois différentes sortes de déclarations d'assertion qui peuvent être créées par une autorité SAML. Toutes les déclarations définies en SAML sont associées à un sujet. Les trois sortes de déclaration définies dans la Recommandation UIT-T X.1141 sont:

- authentification: le sujet de l'assertion a été authentifié par un moyen particulier à un moment précis;
- attribut: le sujet de l'assertion est associé aux attributs fournis;
- décision d'autorisation: une demande d'autorisation du sujet de l'assertion à accéder aux ressources spécifiées a été accordée ou refusée.

La Recommandation UIT-T X.1141 définit également un protocole par lequel les clients peuvent demander des assertions à des autorités SAML et obtenir d'elles une réponse. Ce protocole, qui consiste en formats de messages de demande et de réponse fondés sur XML, peut être lié à de nombreux protocoles sous-jacents de communication et de transport différents. En créant leurs réponses, les autorités SAML peuvent utiliser diverses sources d'information, comme des mémoires de politique externes et des assertions reçues en entrée dans des demandes.

Un ensemble de profils a été défini pour prendre en charge la connexion unique (SSO, *single sign-on*) des navigateurs et autres dispositifs des clients. La Figure 51 illustre le schéma de base pour la réalisation de SSO.

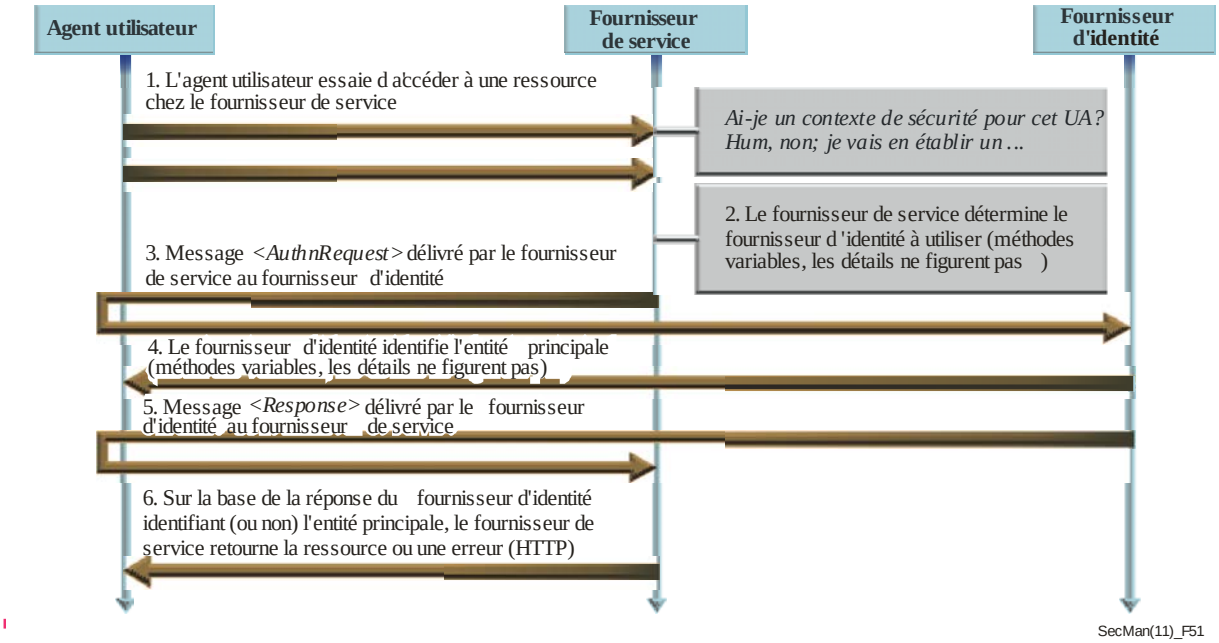


Figure 51 – Schéma de base pour la réalisation de SSO

10.4.2 Langage de balisage extensible de contrôle d'accès

Le langage de balisage extensible de contrôle d'accès (XACML, *eXtensible Access Control Markup Language*) est un vocabulaire XML utilisé pour exprimer les politiques de contrôle d'accès. Le contrôle d'accès consiste à décider si l'accès à une ressource demandée devrait être autorisé et à appliquer cette décision. La Recommandation UIT-T X.1142 définit le cœur de XACML, y compris la syntaxe du langage, les modèles, le contexte avec le modèle de langage de politique, les règles de syntaxe et de traitement. Pour améliorer la sécurité des échanges de politiques fondées sur XACML, la Recommandation UIT-T X.1142 spécifie aussi un profil de signature numérique XML de XACML pour sécuriser les données. Un profil de confidentialité est spécifié afin de fournir des lignes directrices pour la mise en oeuvre. XACML convient pour divers environnements d'application.

10.5 Services par étiquette

Les étiquettes d'identification (notamment les étiquettes RFID) sont largement utilisées mais les préoccupations sont de plus en plus grandes quant au risque d'atteinte à la vie privée. Ceci s'explique en partie par le fait que la technologie RFID permet de collecter et de traiter automatiquement des données et qu'il existe un risque de divulgation délibérée ou accidentelle d'informations sensibles et/ou personnelles.

S'agissant des applications qui utilisent, ou s'appuient sur l'identification par étiquette et qui font intervenir des informations personnelles (soins de santé, passeports, permis de conduire, etc.), la question de la confidentialité est de plus en plus importante.

Au niveau des universités et de l'industrie, la plupart des efforts pour élaborer des mécanismes de protection des informations d'identification personnelle (PII, *personnaly identifiable information*) ont porté sur l'élaboration de protocoles d'authentification entre l'étiquette ID et le terminal ID. Toutefois, ces efforts ne permettent pas de résoudre complètement les problèmes car le serveur dans le domaine du réseau contient toujours des informations utiles relatives à l'identificateur. Une solution consiste à utiliser un mécanisme de protection des informations PII qui soit fonction du profil.

La Recommandation UIT-T X.1171 porte sur les menaces qui pèsent sur les informations PII dans un environnement entreprise-client (B2C, *business-to-customer*) dans lequel les applications utilisent l'identification par étiquette. Elle énonce les exigences pour la protection des informations PII dans un tel environnement et définit la protection des informations PII fondée sur un profil de politiques PII définies par l'utilisateur.

Les applications B2C utilisant l'identification par étiquette peuvent se classer en trois types, comme suit:

a) *L'utilisateur du dispositif est le client*: Dans ce type de service, le client extrait les informations en utilisant un dispositif de lecture mobile. La Figure 52 montre un modèle de base de ce type d'application, se composant de deux opérations de base sur le réseau: la résolution ID et l'extraction du contenu. La résolution ID est la procédure consistant à traduire ou à résoudre un identificateur en une adresse. Le terminal mobile doté d'un dispositif de lecture commence par résoudre un identificateur, qu'il a reçu en provenance de l'étiquette ID via un service d'annuaire, avant d'exécuter une opération d'extraction du contenu sur le réseau.

Figure 52 – Modèle de base d'une application B2C utilisant l'identification par étiquette

b) *L'utilisateur de l'étiquette ID est le client*: Un exemple type de cette application B2C utilisant l'identification par étiquette concerne le contrôle d'accès et/ou l'authentification, par exemple le contrôle des entrées, les passeports, les permis ou le service après-vente. Dans ce type d'application, les dispositifs de lecture peuvent être intégrés dans des terminaux fixes ou mobiles. Le client présente l'étiquette ID (par exemple, sur un passeport ou un ticket) pour bénéficier du service.

c) *Le client est à la fois utilisateur de l'étiquette ID et du dispositif*: Dans le service d'extraction des informations relatives à des produits, le client devient aussi utilisateur de l'étiquette après avoir acquis le produit étiqueté et lu les informations relatives au produit avec son terminal mobile. Un autre exemple peut être un service dans le domaine des soins de santé déclenché par une carte de patient dotée d'une étiquette ID. Dans cette application, de nombreux types de clients pourraient utiliser l'étiquette ID (par exemple le patient, le médecin, l'infirmière). L'utilisateur de l'étiquette ID peut consulter son propre dossier médical grâce au terminal mobile doté d'un dispositif de lecture en lisant sa carte de patient qui est dotée d'une étiquette ID.

Pour les applications B2C qui utilisent l'identification par étiquette, il existe deux principaux risques d'atteinte aux informations PII:

- Fuite d'informations associées à l'identificateur: Dans ce cas, le pirate peut lire des informations de l'étiquette ID sans que l'utilisateur du produit étiqueté le sache. Le pirate lit tout d'abord un identificateur émis par l'étiquette ID que porte l'utilisateur, puis il résout l'identificateur et demande au service d'annuaire la localisation des informations. Enfin, il demande des informations associées à l'étiquette ID.

- Fuite des données relatives au contexte historique: Le pirate peut extraire des données sur l'utilisateur (préférences, habitudes, centres d'intérêt, etc.) à partir des données relatives au contexte historique associées à l'étiquette ID. Il peut utiliser ce type de données à des fins illicites ou commerciales sans le consentement de l'utilisateur.

La Recommandation UIT-T X.1171 décrit les exigences techniques visant à protéger les informations PII dans des applications B2C:

- *Gestion des informations PII par l'utilisateur d'étiquette ID*: L'utilisateur d'étiquette ID doit être à même de gérer ou d'actualiser les informations PII associées à son étiquette ID sur le réseau. Il peut ainsi déterminer quelles informations PII devraient être supprimées ou conservées dans l'application.

- *Authentification pour un utilisateur d'étiquette ID et/ou un utilisateur de dispositif*: Le serveur d'application est tenu d'offrir une procédure d'authentification de l'utilisateur d'étiquette ID, et il peut au besoin offrir une procédure d'authentification de l'utilisateur du dispositif (certaines applications utilisant l'identification par étiquette n'ont pas à authentifier l'utilisateur).

- *Contrôle d'accès aux informations PII d'un utilisateur d'étiquette ID dans un serveur d'application*: Le serveur d'application est tenu de contrôler l'accès aux informations PII de l'utilisateur d'étiquette ID.

- *Confidentialité des informations associées à une étiquette ID*: Le serveur d'application est tenu d'assurer la confidentialité des données pour faire en sorte que les informations associées à une étiquette ID ne puissent pas être lues par des utilisateurs non autorisés.

- *Consentement en vue de la collecte de données de journalisation relatives à l'utilisateur du dispositif*: Le serveur d'application peut offrir une procédure de consentement pour la collecte de données de journalisation relatives à l'utilisateur du dispositif si ce type de collecte est nécessaire pour l'application.

L'exemple qui suit illustre un service de protection des informations PII (PPS) basé sur le profil de politiques PII de l'utilisateur. Le scénario de service pour le PPS correspond en général à une procédure de personnalisation par étiquette, comme dans le cas de l'achat d'un produit étiqueté. La Figure 53 illustre le flux général de service PPS pour l'application utilisant l'identification par étiquette.

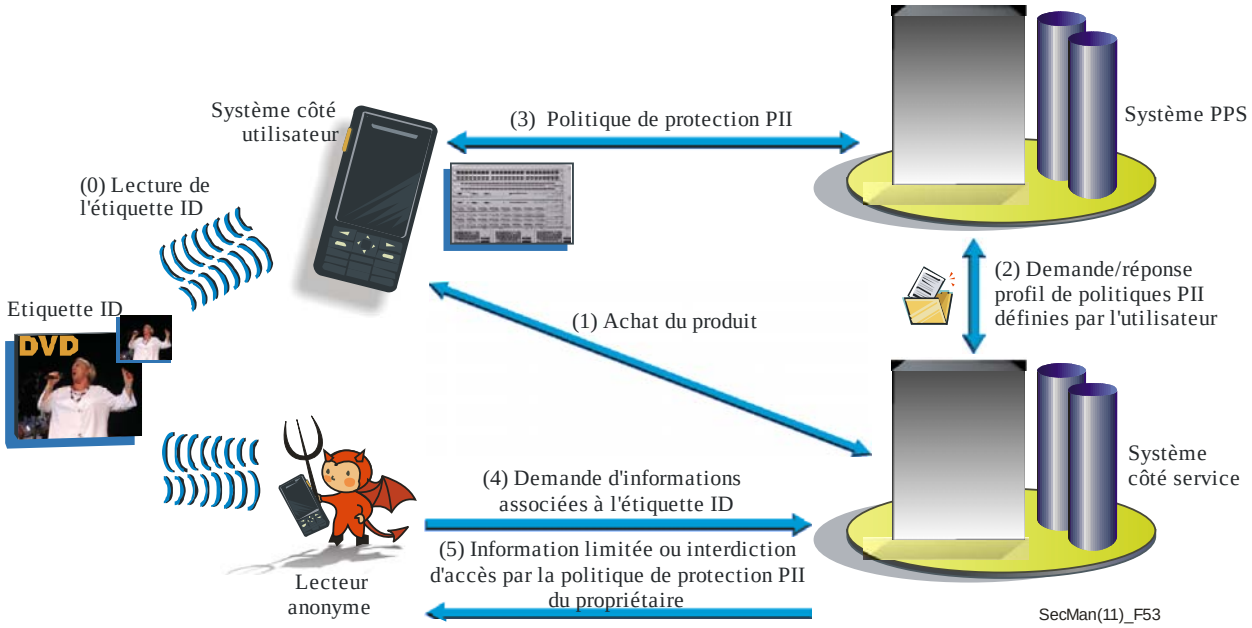


Figure 53 – Flux général de service de protection des informations PII (PPS)

0) Un consommateur lit l'identificateur du produit étiqueté à l'aide de son terminal mobile équipé d'un lecteur.

1) Le consommateur consulte les informations sur le produit à partir du réseau de services d'application, puis achète le produit en utilisant l'une des diverses méthodes de paiement. A ce moment, le consommateur devient l'utilisateur de l'étiquette ID.

2) L'application utilisant l'identification par étiquette demande ensuite au système PPS de lui fournir le profil de politiques PII définies par l'utilisateur, le système fournissant alors à l'application le profil PII en question.

3) Le système PPS reçoit le profil de politiques de protection des informations PII de l'utilisateur pour cette application.

4) N'importe qui peut demander au système côté service les informations associées à cette étiquette ID.

5) Le demandeur peut consulter toutes les informations fournies par le système côté service s'il est l'utilisateur de l'étiquette ID. Sinon, soit le demandeur ne peut pas accéder à une quelconque information, soit il obtient des informations limitées.

11. Lutte contre les menaces courantes dans les réseaux

11 Lutte contre les menaces courantes dans les réseaux

Les menaces qui pèsent sur les systèmes informatiques et sur les réseaux qui les interconnectent sont nombreuses et variées. De nombreuses attaques peuvent être déclenchées localement, mais aujourd'hui, la grande majorité des attaques sont réalisées via des réseaux de communications. Le fait que les ordinateurs et les dispositifs de réseau soient toujours plus nombreux à être raccordés à l'Internet et à être utilisés à domicile et au travail par des personnes peu formées ou peu informées sur la sécurité informatique augmente considérablement la facilité et la probabilité des attaques distantes, souvent aveugles. On observe une prolifération rapide des spams, logiciels espions, virus et autres vecteurs d'attaques, les attaquants profitant souvent de la faiblesse ou de la protection insuffisante des systèmes pour diffuser leurs logiciels malveillants.

Le présent chapitre donne un aperçu des travaux menés par l'UIT-T pour lutter contre certaines de ces menaces.

11.1 Le spam

Le spam est un message indésirable, non sollicité et potentiellement dangereux. Si le spam par courrier électronique est le type de spam le plus répandu, le phénomène est également observé sur d'autres voies de communication comme la messagerie instantanée, la messagerie mobile et la VoIP. Par conséquent, la définition de ce terme évolue et s'élargit à mesure que se développent les technologies qui offrent autant de nouvelles possibilités de créer des spams. Le spam, qui interfère avec les opérations légitimes des opérateurs de télécommunication, des fournisseurs de services et des utilisateurs est considéré comme un problème de grande ampleur. Il consomme une certaine largeur de bande et des cycles de traitement et, dans les cas extrêmes, peut conduire à des attaques par déni de service résultant de l'inondation des réseaux. Si aucune mesure antispam n'est efficace isolément, la mise en œuvre de mesures combinées ne débouche souvent que sur la réduction du volume de spams, tant les spammeurs font preuve d'agilité et d'ingéniosité. Différentes mesures sont mises en œuvre, parmi lesquelles la réglementation, les mesures techniques, la coopération internationale et les campagnes de sensibilisation auprès des utilisateurs et des fournisseurs de service Internet.

11.1.1 Stratégies techniques de lutte contre le spam

Les travaux menés par l'UIT-T dans le domaine du spam consistent essentiellement à mettre au point des mesures techniques pour lutter contre ce phénomène. Le cadre utilisé pour l'élaboration des Recommandations prévoit des possibilités d'élargissement, comme le montre la Figure 54.

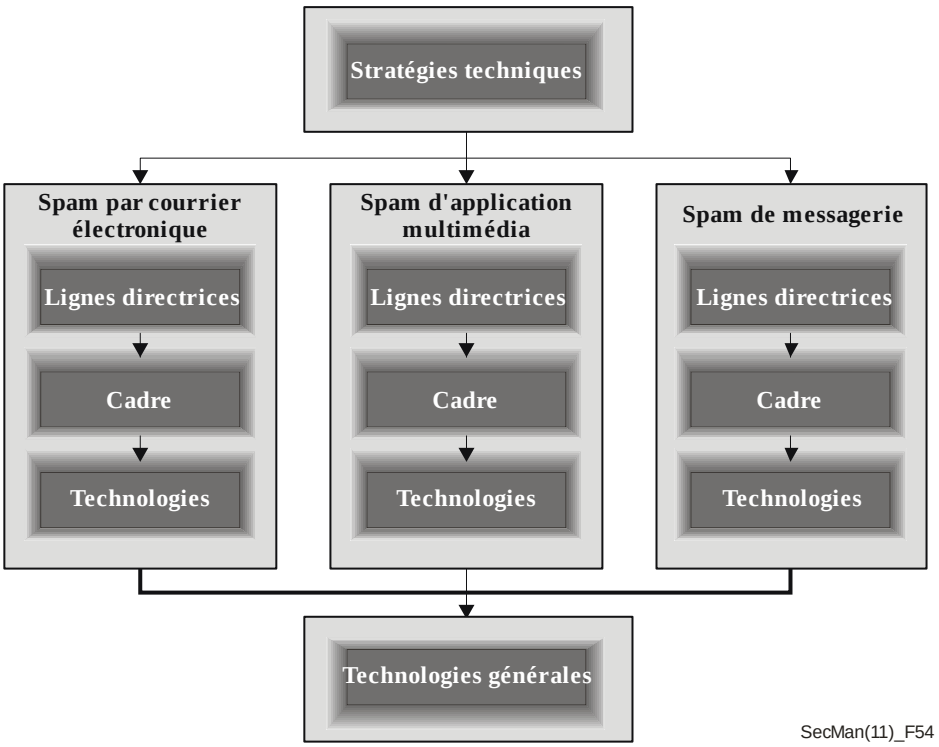


Figure 54 – Cadre de normalisation de la lutte contre le spam

La Recommandation UIT-T X.1231 énonce des stratégies pour lutter contre le spam et sert de point de départ pour les travaux. Elle décrit les différents types de spam et leurs caractéristiques communes et présente les approches techniques pour lutter contre le spam. Elle propose aussi un modèle général qui peut être utilisé pour mettre au point une stratégie antispam efficace.

Il s'agit d'un modèle hiérarchique dans lequel cinq stratégies sont réparties dans trois couches. Les relations entre les stratégies sont illustrées dans la Figure 55. Il ressort de ce modèle que les stratégies dépendent largement les unes des autres mais, dans certains cas, il est possible que les stratégies ne soient pas toutes retenues pour des raisons financières. En outre, le modèle doit être adapté aux besoins de chaque scénario d'application particulier.

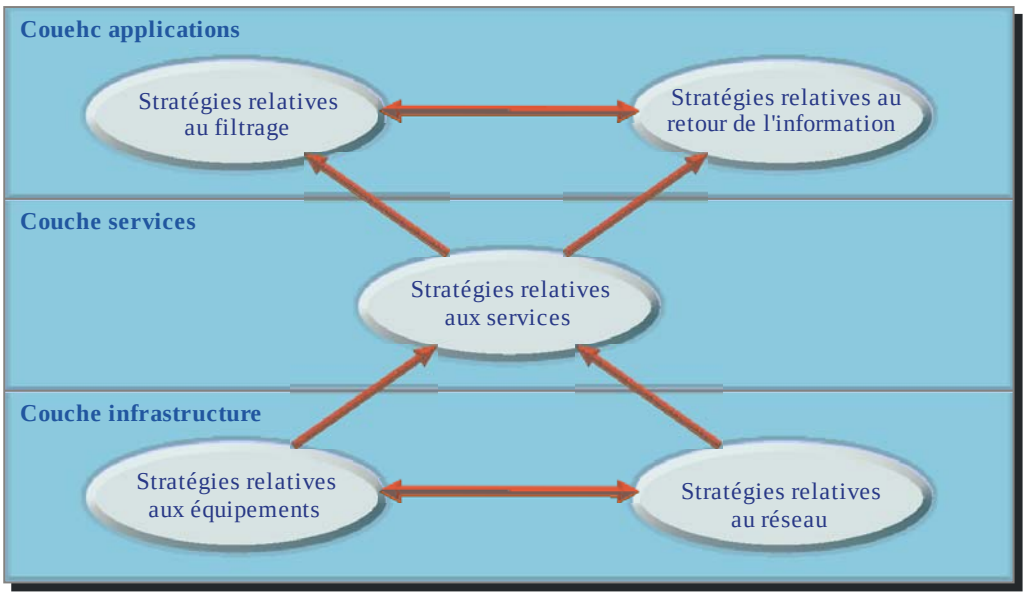


Figure 55 – Modèle général de lutte contre le spam

11.1.2 Spam par courrier électronique

Le spam par courrier électronique est le type de spam le plus répandu. Il pose des difficultés techniques complexes et les solutions mises en œuvre pour en venir à bout doivent s'appuyer sur des mesures techniques appropriées. Si la puissance publique et la législation jouent un rôle essentiel, leur action est insuffisante pour résoudre les difficultés que pose le spam par courrier électronique. Le problème est d'autant plus complexe qu'il est difficile d'identifier le spammeur lorsque le protocole SMTP est utilisé.

Deux Recommandations ont pour objet de faciliter la lutte contre le spam par courrier électronique. La Recommandation UIT-T X.1240 s'adresse aux utilisateurs qui souhaitent développer des solutions techniques de lutte contre le spam par courrier électronique. Elle spécifie les concepts fondamentaux, les caractéristiques, les effets et les problèmes techniques associés à la lutte contre le spam par courrier électronique. Elle présente en outre les solutions techniques existantes et les activités connexes réalisées par diverses organisations de normalisation et par d'autres groupes qui travaillent à la lutte contre le spam par courrier électronique.

La Recommandation UIT-T X.1241 décrit une structure recommandée d'un domaine de traitement antispam et définit la fonction des principaux modules de ce domaine. Le cadre établit un mécanisme de partage des informations sur les spams par courrier électronique entre les différents serveurs de messagerie électronique. Il vise à promouvoir une plus grande coopération entre les fournisseurs de services dans la lutte contre le spam et, en particulier, à mettre en œuvre une méthode de communication d'alertes lorsqu'un spam est identifié. Un autre document, le *Supplément 6 aux Recommandations UIT-T de la série X* présente les instances internationales qui s'intéressent au spam et contient une étude de cas.

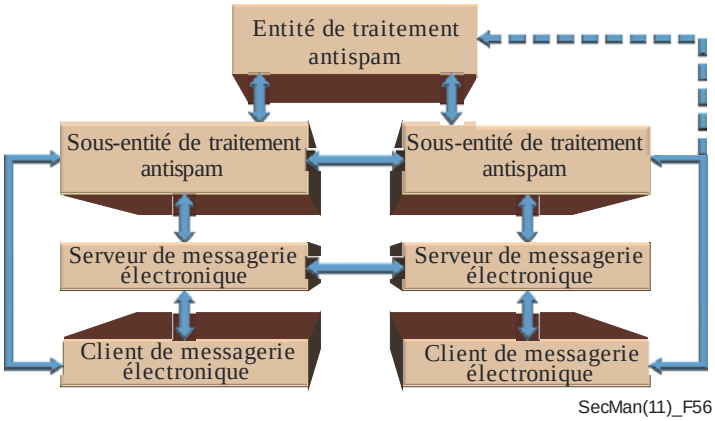


Figure 56 – Structure générale du domaine de traitement antispam applicable au spam par courrier électronique

La Figure 56 illustre les processus du cadre de la Recommandation UIT-T X.1241. L'entité de traitement antispam est située dans un système indépendant tandis que les sous-entités sont situées dans un ou plusieurs fournisseurs de service de messagerie électronique. L'entité de traitement communique de nouvelles règles aux sous-entités, qui doivent les vérifier et les parfaire. Il existe aussi une fonction qui permet de résoudre les éventuels conflits entre les règles.

11.1.3 Spam d'application multimédia IP

La Recommandation UIT-T X.1244 spécifie les concepts de base, les caractéristiques et les aspects techniques liés à la lutte contre le spam dans les applications multimédias IP (téléphonie IP, messagerie instantanée, etc.). Elle propose une classification des différents types de spams d'application multimédia IP et en détaille les caractéristiques. Elle décrit également diverses menaces de sécurité que présente le spam d'application multimédia IP et indique les aspects à prendre en considération pour lutter contre ce type de spam. Certaines techniques mises au point pour limiter le spam par courrier électronique peuvent être utilisées dans le cas du spam d'application multimédia IP. La Recommandation UIT-T X.1244 analyse les mécanismes classiques de lutte contre le spam et étudie leur applicabilité dans le cas du spam d'application multimédia IP.

Les techniques antispam peuvent être appliquées au spam multimédia IP en fonction des caractéristiques spécifiques de ce dernier. Le Tableau 8 présente la classification utilisée dans la Recommandation UIT-T X.1244.

Tableau 8 – Classification des spams d'application multimédia IP

	Texte	Voix	Vidéo
En temps réel	• spam de messagerie instantanée • spam de bavardage	• spam de VoIP • spam de messagerie instantanée	• spam de messagerie instantanée
Pas en temps réel	• spam de messagerie multimédia/textuelle • spam textuel de service de partage de fichier P2P • spam textuel de site web	• spam de messagerie multimédia/vocale • spam vocal de service de partage de fichier P2P • spam vocal de site web	• spam de messagerie multimédia/vidéo • spam vidéo de service de partage de fichier P2P • spam vidéo de site web

La Recommandation UIT-T X.1245 décrit le cadre général de lutte contre le spam dans les applications multimédias IP comme la téléphonie IP, la messagerie instantanée et les conférences multimédias.

La Figure 57 illustre le cadre de lutte contre le spam dans les applications multimédias IP. Ce cadre comporte quatre groupes de fonctions antispam, à savoir les fonctions antispam centrales (CASF), les fonctions antispam côté destinataire (RASF), les fonctions antispam côté expéditeur (SASF) et les fonctions du destinataire de spams (SRF). Cette Recommandation décrit les fonctionnalités et les interfaces de chaque fonction pour la lutte contre le spam multimédia IP.

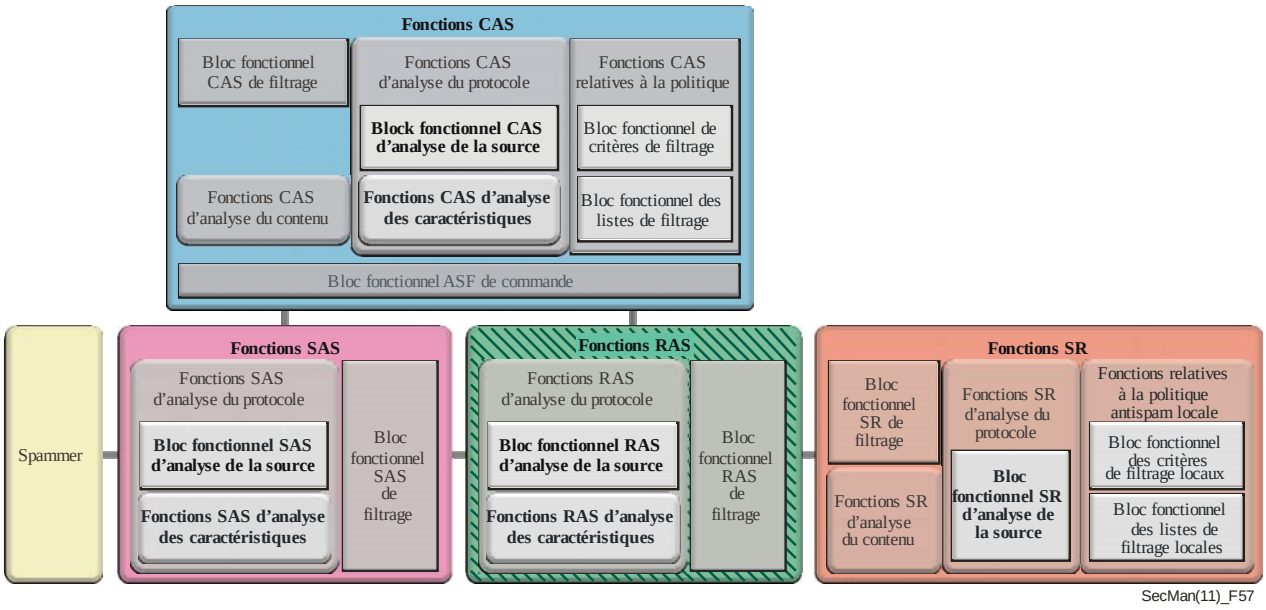


Figure 57– Cadre de lutte contre le spam multimédia IP

Le Supplément 11 aux Recommandations UIT-T de la série X décrit un cadre technique de lutte contre le spam de VoIP fondé sur l'utilisation de listes de blocage en temps réel (RBL). La Figure 58 illustre les quatre entités fonctionnelles de ce cadre: le système de prévention des spams de VoIP (VSPS), le serveur de politique de prévention des spams de VoIP (VSPPS), le système central RBL de prévention des spams de VoIP (VSP-RBL) et le système de réputation des utilisateurs (URS). Ce Supplément spécifie en outre, pour chaque entité fonctionnelle, les fonctionnalités, les procédures et les interfaces utilisées pour combattre le spam de VoIP.

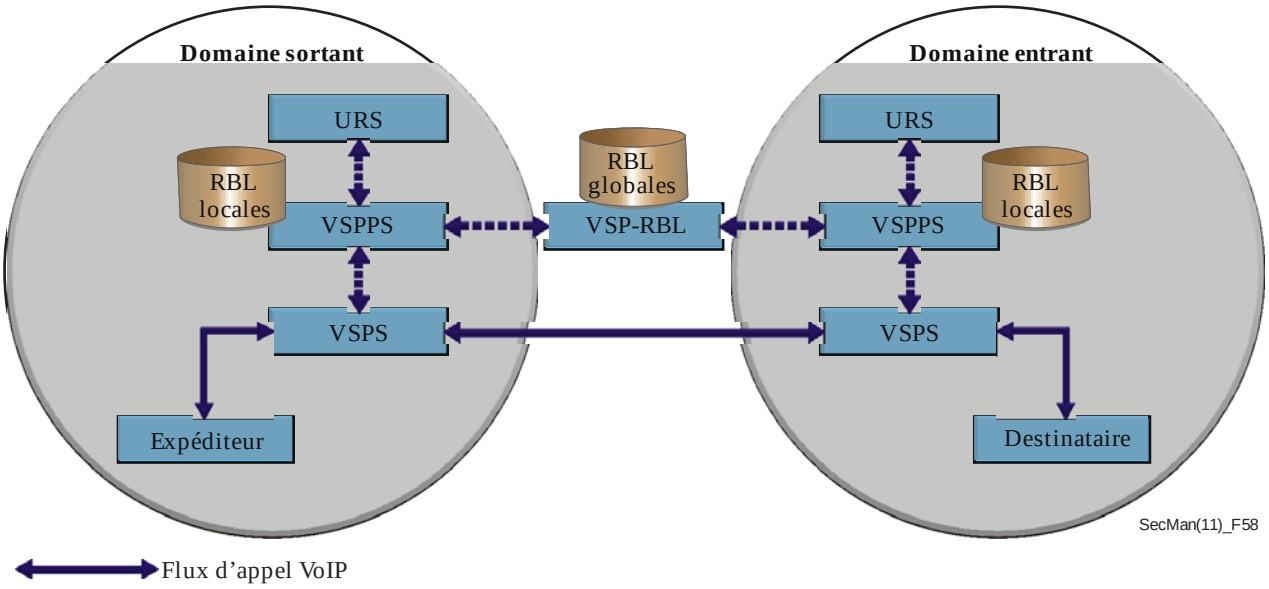


Figure 58 – Architecture fonctionnelle de lutte contre le spam de VoIP

11.1.4 Spam de messagerie mobile

L'expression "spam de messagerie mobile" couvre à la fois le spam du service de message court (SMS) et le spam du service de messagerie multimédia (MMS). La Recommandation UIT-T X.1242 définit la structure et les fonctions du système de filtrage du spam du service SMS, la gestion du service fourni à l'utilisateur, les protocoles de communication et les exigences fonctionnelles de base des terminaux dotés de fonctions SMS. Elle définit aussi des méthodes permettant aux utilisateurs de gérer (rechercher, supprimer ou restituer) les messages courts filtrés. Le filtrage peut être fondé sur des caractéristiques telles que l'adresse, le numéro de téléphone, l'heure ou le contenu. Les exigences relatives au logiciel du terminal assurant le filtrage du spam du service SMS sont énoncées dans un appendice à la Recommandation UIT-T X.1242.

11.1.5 Système de passerelle interactive pour lutter contre le spam

La collaboration sur le plan technologique est considérée comme un élément clé de la lutte contre le spam. La Recommandation UIT-T X.1243 décrit le système de passerelle interactive comme un moyen technique de lutte contre le spam interdomaines. Ce système permet la notification des spams entre différents domaines et empêche le trafic de spam de passer d'un domaine à un autre. Cette Recommandation spécifie l'architecture du système de passerelle, décrit les entités, protocoles et fonctions de base de ce système et présente des mécanismes de détection du spam, de partage d'informations et des actions spécifiques pour lutter contre le spam.

11.2 Codes malveillants, logiciels espions et logiciels trompeurs

Bien que les codes malveillants (virus, vers, chevaux de Troie, etc.) soient sans doute ceux qui présentent le plus de risques pour les systèmes et les réseaux, les logiciels espions et autres logiciels trompeurs (c'est-à-dire les logiciels qui effectuent des opérations non autorisées) constituent également une menace importante. Si les organisations et les individus ne mettent pas en œuvre toute une série de mesures proactives (pare-feu, mesures antivirus, mesures anti-logiciel espion) contre ces menaces, il est presque certain que leurs systèmes ou réseaux seront compromis. Toutefois, les contre-mesures disponibles n'ont pas toutes la même efficacité et ne sont pas toujours complémentaires.

Dans de nombreux pays, les régulateurs exigent de plus en plus que les fournisseurs de services apportent des garanties concernant les mesures de sécurité et de sûreté qu'ils ont prises, et qu'ils aident davantage les utilisateurs à utiliser l'Internet en toute sécurité.

Le Supplément 9 aux Recommandations UIT-T de la série X fournit des lignes directrices pour la réduction des logiciels malveillants dans les réseaux TIC.

La Recommandation UIT-T X.1207 est une norme visant à:

a) promouvoir, dans le cadre des services d'hébergement de pages web, les meilleures pratiques fondées sur les principes suivants: obligation d'informer clairement les utilisateurs, nécessité d'obtenir leur consentement et possibilité pour eux d'exercer un contrôle; et

b) promouvoir les meilleures pratiques (par le biais des fournisseurs de services de télécommunication) à l'intention des particuliers sur l'utilisation sûre et sécurisée des ordinateurs personnels et de l'Internet.

La Recommandation UIT-T X.1207 donne aux fournisseurs de services des indications claires sur la gestion des risques de sécurité, l'utilisation de produits sûrs et sécurisés, la surveillance du réseau et les interventions nécessaires, l'assistance, la mise à jour en temps utile et l'hébergement sécurisé de pages web. Des conseils sont donnés pour guider et sensibiliser les utilisateurs et pour adopter des mesures techniques de protection des utilisateurs finals. Un appendice, qui ne fait pas partie intégrante de la Recommandation, contient des liens vers d'autres ressources.

11.3 Notification et diffusion de mises à jour des logiciels

Un code malveillant peut se propager avec une rapidité alarmante. Par conséquent, même si des mesures de protection avancées sont adoptées, la vitesse de propagation des nouvelles menaces est telle que les systèmes et les réseaux qui ne contiennent pas les dernières mises à jour sont vulnérables. Les systèmes sont également particulièrement vulnérables aux "zero-day exploits" (c'est-à-dire aux menaces nouvelles ou auparavant inconnues pour lesquelles aucune signature antivirus ou aucun correctif n'a encore été élaboré). Dans cet environnement, la distribution et l'installation rapides des mises à jour est essentielle. Cependant, il existe un certain nombre de problèmes associés à la distribution et à l'installation de ces mises à jour.

La plupart des logiciels du commerce, notamment les systèmes d'exploitation et les systèmes conçus pour assurer une protection de sécurité (antivirus, anti-logiciel espion, pare-feu, etc.), contiennent une fonctionnalité qui permet une mise à jour automatique. Toutefois, cette fonctionnalité doit être activée par l'utilisateur. Lorsqu'un utilisateur est simplement informé du fait que des mises à jour sont disponibles (ou éventuellement du fait que des mises à jour ont été téléchargées), il doit prendre des mesures pour permettre le téléchargement et/ou l'installation de ces mises à jour. De nombreuses mises à jour nécessitent un redémarrage des systèmes après installation, ce que les utilisateurs individuels ne font pas nécessairement immédiatement. Les organisations qui disposent d'un programme de sécurité bien géré procèdent généralement à une gestion centrale des mises à jour et imposent les mises à jour des systèmes des

utilisateurs finals. En revanche, la mise à jour des systèmes individuels (par exemple ordinateurs à la maison) et la mise à jour des systèmes dans les petites organisations sont généralement peu méthodiques.

Un autre problème se pose avec les mises à jour courantes: les fournisseurs de logiciels n'utilisent pas de pratiques uniformes pour avertir les utilisateurs de la disponibilité de mises à jour ou des conséquences possibles en cas de non-installation des mises à jour. Ils n'utilisent pas non plus de méthode uniforme pour tenir les utilisateurs informés des bonnes pratiques les plus récentes pour préserver la sécurité des logiciels. Enfin, il n'existe pas de méthode uniforme pour la notification des problèmes détectés par les utilisateurs après l'installation d'une mise à jour.

La Recommandation UIT-T X.1206 examine les difficultés rencontrées pour tenir à jour les logiciels et décrit un cadre indépendant du fournisseur pour faire face aux problèmes. Une fois qu'un actif est enregistré, les dernières informations de vulnérabilité et les correctifs ou mises à jour peuvent être diffusés automatiquement aux utilisateurs ou directement dans les applications. La Recommandation UIT-T X.1206 définit un cadre que tout fournisseur peut utiliser pour la notification ainsi que pour fournir des informations de vulnérabilité et diffuser les correctifs ou mises à jour nécessaires. Elle définit aussi le format des informations qu'il convient d'utiliser dans les composants et entre eux.

La Recommandation UIT-T X.1206 permet aux administrateurs de système de connaître la situation de tout actif dont ils sont responsables. Elle décrit les problèmes de préservation des actifs du point de vue de leur identification, ainsi que du point de vue de la diffusion des informations et de la gestion des systèmes/du réseau. Elle contient aussi une description de la sécurité qui devrait être prise en considération dans le cadre indépendant du fournisseur.

La Recommandation UIT-T X.1206 définit les structures de données des composants qui sont nécessaires pour ces activités, y compris le schéma XML associé, et donne le format des informations qu'il convient d'utiliser dans les composants de ce cadre et entre les composants.

12. L'avenir de la normalisation de la sécurité des TIC

12 L'avenir de la normalisation de la sécurité des TIC

L'Union télégraphique internationale, ancêtre de l'UIT, a été créée en 1865. Si, à l'origine, son champ de compétences était le télégraphe, l'UIT mène aujourd'hui des travaux sur l'ensemble du secteur des TIC, de la radiodiffusion numérique à l'Internet en passant par les technologies mobiles et la télévision 3D. L'élaboration de normes sur les TIC s'est nettement accélérée ces dernières années compte tenu de la croissance rapide de l'utilisation de l'Internet et d'autres réseaux et de la nécessité de protéger les utilisateurs et les systèmes contre des menaces de sécurité toujours plus nombreuses et variées.

Le présent Manuel a présenté de façon générale certaines initiatives et réalisations essentielles des Commissions d'études de l'UIT-T dans le domaine de la sécurité afin de mieux faire connaître les activités et les difficultés techniques auxquelles les utilisateurs et les responsables de la mise en œuvre des réseaux sont confrontés. Les lecteurs sont invités à consulter les nombreuses ressources mises en ligne par l'UIT-T pour obtenir plus de détails sur les aspects présentés ici et à utiliser les Recommandations et les documents d'information afin de contribuer à créer un environnement en ligne plus sûr et d'améliorer la confiance des utilisateurs dans les opérations en ligne.

A l'avenir, la convergence des réseaux de télécommunication et des réseaux informatiques va se poursuivre. Les applications de réseaux et les applications de services fondées sur le web vont continuer à croître rapidement et à gagner de l'importance, mais les menaces vont, elles aussi, continuer à évoluer. Aussi la conception et l'élaboration de mesures efficaces pour lutter contre ces menaces, de même que la conception et la mise en place de systèmes et de réseaux plus sécurisés en vue de réduire les vulnérabilités intrinsèques resteront-elles des défis. Cependant, le partage d'informations sur les menaces, comme le montrent nos activités relatives à l'échange d'informations sur la cybersécurité, permettra à la communauté mondiale des télécommunications/TIC de mieux répondre aux menaces et de diminuer leur incidence.

Les 193 Etats Membres et les quelque 700 Membres de Secteur et Associés de l'UIT continueront à relever ces défis en élaborant des Recommandations techniques et des lignes directrices sur la sécurité dans le cadre d'un programme de travail ambitieux dicté par les besoins des membres et guidé par la structure organisationnelle établie par l'Assemblée mondiale de normalisation des télécommunications. Chaque fois qu'il le pourra, l'UIT-T collaborera avec d'autres organisations de normalisation pour éviter la redondance des tâches et parvenir à des solutions harmonisées aussi efficacement et rapidement que possible.

13. Sources d'informations complémentaires

13 Sources d'informations complémentaires

Le présent Manuel contient un aperçu général des travaux de l'UIT-T sur la sécurité. Des informations beaucoup plus détaillées et de nombreuses normes sont disponibles gratuitement sur le site web de l'UIT-T.

13.1 Aperçu des travaux de la CE 17

En premier lieu, il convient de préciser que la page d'accueil de la CE 17 de l'UIT-T contient des liens vers des informations relatives aux activités de la CE 17 (exposés, résumés de Recommandations en cours d'élaboration, noms des principales personnes). Les liens vers la Commission d'études directrice sur la sécurité des télécommunications et vers la Commission d'études directrice sur la gestion d'identité (IdM) donnent des informations sur les activités et les résultats des travaux de ces deux entités.

13.2 Recueil sur la sécurité

Le recueil contient des informations sur les Recommandations de l'UIT, des informations connexes et des informations sur les activités de l'UIT dans le domaine de la sécurité. Il comprend cinq parties, chacune d'elles pouvant être téléchargée. Ces parties sont les suivantes:

- Catalogue des Recommandations approuvées relatives à la sécurité des télécommunications, qui comprend les Recommandations portant expressément sur la sécurité et celles qui décrivent ou utilisent des fonctions utiles pour la sécurité.

- Liste des définitions relatives à la sécurité approuvées par l'UIT-T extraites des Recommandations UIT-T approuvées.

- Présentation succincte des Commissions d'études de l'UIT-T menant des acticités dans le domaine de la sécurité.

- Présentation succincte des Recommandations faisant l'objet, au sein des Commissions d'études de l'UIT-T, d'un examen relatif aux considérations de sécurité.

- Présentation succincte des autres activités de l'UIT dans le domaine de la sécurité.

13.3 Feuille de route sur les normes de sécurité

La feuille de route sur les normes de sécurité est une ressource en ligne qui donne des informations sur les normes existantes relatives à la sécurité des TIC et sur les travaux en cours dans les principales organisations de normalisation. Outre les activités de l'UIT-T dans le domaine de la sécurité, la feuille de route contient des informations sur les activités de normalisation de la sécurité menées par l'ISO/CEI, l'ATIS, l'ENISA, l'ETSI, l'IEEE, l'IETF, OASIS, le 3GPP et le 3GPP2.

Le feuille de route comprend six parties directement accessibles en ligne:

- Partie 1, *Organisations s'occupant de normalisation des TIC et leurs activités*, qui contient des informations sur la structure de la feuille de route et sur chacune des organisations de normalisation répertoriées. La Partie 1 contient aussi des liens vers les glossaires et vocabulaires existants relatifs à la sécurité.

- Partie 2, *Normes approuvées relatives à la sécurité des TIC*, qui contient une base de données des normes de sécurité approuvées proposant des liens directs vers la plupart des normes, dans laquelle il est possible de faire des recherches.

- Partie 3, *Normes de sécurité en cours d'élaboration*.
- Partie 4, *Besoins futurs et propositions de nouvelles normes de sécurité.*
- Partie 5: *Bonnes pratiques en matière de sécurité*.
- Partie 6, Situation en ce qui concerne la gestion d'identité (IdM): normes IdM, organisations et analyse des lacunes dans ce domaine.

13.4 Lignes directrices pour la mise en œuvre de la sécurité

Le Supplément 3 aux Recommandations UIT-T de la série X contient plus de détails sur certains aspects examinés dans le présent Manuel et énonce des lignes directrices pour la mise en œuvre de la sécurité dans les systèmes et dans les réseaux qui peuvent être utilisées pour réaliser un programme de sécurité de réseau. Quatre domaines sont traités: politique de sécurité technique; identification des actifs; menaces, vulnérabilités et solutions pour y remédier; et évaluation de la sécurité. Ce document indique les principaux éléments nécessaires pour établir et gérer la politique technique nécessaire pour la gestion des réseaux qui peuvent être exploités par plusieurs opérateurs et qui contiennent des produits et des systèmes provenant de multiples fournisseurs. Il énonce aussi des lignes directrices relatives à des questions réglementaires.

13.5 Informations complémentaires sur l'annuaire

Pour plus d'informations sur les Recommandations de la série UIT-T X.500, la source d'informations faisant autorité est la série de Recommandations UIT-T X.500 proprement dite. On trouvera d'autres informations didactiques et un guide de mise en œuvre à l'adresse: www.x500standard.com.

Des informations sur l'authentification d'utilisateur sont disponibles à l'adresse: http://www.x500standard.com/index.php?n=X509.X509ProtectingDirectory.

Des informations sur le contrôle d'accès sont disponibles à l'adresse: http://www.x500standard.com/index.php?n=X500.AccessControl.

Une description plus détaillée des fonctionnalités de confidentialité des données UIT-T X.500 est disponible à l'adresse: http://www.x500standard.com/index.php?n=X500.DataPrivacyProtection.

Des éléments didactiques en ligne sur la Recommandation UIT-T X.500 sont disponibles à l'adresse: http://www.x500standard.com/index.php?n=Participate.Tutorial.

Les livres blancs sur la Recommandation UIT-T X.500 sont disponibles à l'adresse: http://www.x500standard.com/index.php?n=Participate.Whitepapers.

Annexe A

Définitions relatives à la sécurité

Annexe A

Définitions relatives à la sécurité

Le tableau qui suit contient les définitions des termes employés dans la présente publication. Toutes les définitions sont tirées des Recommandations UIT-T en vigueur. Une liste plus complète de définitions relatives à la sécurité figure dans le recueil des définitions relatives à la sécurité approuvées par l'UIT-T et tenu à jour par la Commission d'études 17.

Terme	Définition	Référence
contrôle d'accès (*access control*)	1) 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. 2) Restriction du flux d'informations provenant des ressources d'un système aux personnes, programmes, processus ou autres ressources de système de réseau autorisés.	UIT-T X.800 UIT-T J.170
liste de contrôle d'accès (*access control list*)	Liste des entités qui sont autorisées à accéder à une ressource, avec leurs autorisations d'accès.	UIT-T X.800
politique de contrôle d'accès (*access control policy*)	Ensemble des règles définissant les conditions dans lesquelles l'accès peut se dérouler.	UIT-T X.812
menaces accidentelles (*accidental threats*)	Menaces qui existent sans qu'il y ait préméditation. Des exemples de menaces accidentelles qui se sont concrétisées sont: défaillance de système, bévues opérationnelles et bogues dans le logiciel.	UIT-T X.800
imputabilité (*accountability*)	Propriété qui garantit que les actions d'une entité ne peuvent être imputées qu'à cette entité.	UIT-T X.800
algorithme (*algorithm*)	Processus mathématique qui peut être utilisé pour l'embrouillage et pour le désembrouillage d'un flux de données.	UIT-T J.93
attaque (*attack*)	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.	UIT-T H.235
attribut (*attribute*)	Dans le cadre de la messagerie, élément d'information, composante d'une liste d'attributs, qui décrit un utilisateur ou une liste de distribution et qui peut aussi se rapporter à la structure physique ou organisationnelle du système de messagerie (ou du réseau qui le supporte).	UIT-T X.400
autorité d'attribut, autorité en charge des attributs (AA, *attribute authority*)	1) Autorité qui attribue des privilèges par l'émission de certificats d'attribut. 2) Entité bénéficiant de la confiance d'une ou de plusieurs entités pour l'établissement et la signature de certificats d'attribut. *Note* – Une autorité de certification peut également être une autorité en charge des attributs.	UIT-T X.509 UIT-T X.842

Terme	Définition	Référence
certificat d'attribut (*attribute certificate*)	Structure de données, portant la signature numérique d'une autorité d'attribut, qui lie certaines valeurs d'attribut à des informations d'identification concernant son détenteur.	UIT-T X.509
authentification (*authentication*)	1) Processus de confirmation d'identité. *Note* – Voir entité principale (*principal*) et vérificateur (*verifier*) et les deux formes d'authentification distinguées (auth. de l'origine des données (*data origin auth.*) + auth. d'identité (*entity auth.*)). L'authentification peut être *unilatérale* ou *mutuelle*. La première atteste l'identité d'une seule entité principale. La seconde atteste l'identité des deux entités principales. 2) Attestation de l'identité revendiquée par une entité. 3) Voir authentification de l'origine des données (*data origin authentication*) et authentification de l'entité homologue (*peer entity authentication*). Le terme authentification n'est pas associé à l'intégrité des données; le terme intégrité des données est utilisé à la place. 4) Corroboration de l'identité des objets se rapportant à l'établissement d'une association. Par exemple, il peut s'agir des entités d'application, des processus d'application et des usagers des applications. *Note* – Ce terme a été défini en vue d'indiquer clairement qu'il s'agit d'une authentification de portée plus large que l'authentification de l'entité homologue dont traite la Recommandation UIT-T X.800 du CCITT. 5) Processus consistant à vérifier l'identité déclarée d'une entité auprès d'une autre entité. 6) Processus destiné à permettre au système de vérifier avec certitude l'identité d'un tiers.	UIT-T X.811 UIT-T X.811 UIT-T X.800 UIT-T X.217 UIT-T J.170 UIT-T J.93
échange d'authentification, échange pour authentification (*authentication exchange*)	1) Mécanisme destiné à garantir l'identité d'une entité par échange d'informations. 2) Séquence d'un ou de plusieurs transferts d'informations d'authentification (AI) pour échange, en vue de réaliser une authentification.	UIT-T X.800 UIT-T X.811
service d'authentification (*authentication service*)	Ce service fournit la preuve qu'un objet ou un sujet possède effectivement l'identité qu'il déclare. Les types d'authentification suivants peuvent être nécessaires en fonction du type d'acteur et du but de l'identification: authentification de l'utilisateur, authentification de l'entité homologue, authentification de l'origine des données. Des exemples de mécanismes utilisés pour implémenter le service d'authentification sont l'authentification simple par mot de passe et numéro d'identification personnel (PIN, *personal identification number*) et l'authentification forte basée sur des méthodes de chiffrement.	UIT-T M.3016.2
autorité (*authority*)	Entité responsable de l'émission de certificats. Deux types sont définis: les autorités de certification émettant des certificats de clé publique et les autorités d'attribut émettant des certificats d'attribut.	UIT-T X.509
autorisation (*authorization*)	1) Attribution de droits, comprenant la permission d'accès sur la base de droits d'accès. *Note* – Cette définition implique que les droits sont des droits d'effectuer certaines activités (telles que l'accès aux données) et qu'ils ont été accordés à une entité, un opérateur humain ou un processus. 2) Octroi d'une permission sur la base d'une identité authentifiée. 3) Fait de donner l'accès à un service ou à un dispositif à quelqu'un qui dispose de la permission d'accès.	UIT-T X.800 UIT-T H.235 UIT-T J.170

Terme	Définition	Référence
disponibilité (*availability*)	Propriété d'être accessible et utilisable sur demande par une entité autorisée.	UIT-T X.800
capacité (*capability*)	Jeton utilisé comme identificateur d'une ressource de telle sorte que la possession du jeton confère des droits d'accès à cette ressource.	UIT-T X.800
certificat (*certificate*)	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 (certificat de sécurité – UIT-T X.810). Ce terme renvoie aux certificats "de 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.	UIT-T H.235
politique de certificat (*certificate policy*)	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.	UIT-T X.509
liste de révocation de certificats (CRL, *certificate revocation list*)	1) 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. 2) Une liste CRL contient les numéros de série des certificats qui ont été révoqués (par exemple parce que la clé a été compromise ou parce que le sujet ne fait plus partie du personnel) et dont la période de validité n'a pas encore expiré.	UIT-T X.509 UIT-T Q.817
autorité de certification (CA, *certification authority*)	1) 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. 2) 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.	UIT-T X.509 UIT-T X.810
cryptogramme, texte chiffré (*ciphertext*)	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.	UIT-T X.800
texte en clair (*cleartext*)	Données intelligibles dont la sémantique est compréhensible.	UIT-T X.800
confidentialité (*confidentiality*)	Propriété d'une information qui n'est ni disponible, ni divulguée aux personnes, entités ou processus non autorisés.	UIT-T X.800
service de confidentialité (*confidentiality service*)	Le service de confidentialité fournit une protection contre la divulgation non autorisée de données échangées. On peut distinguer les types de service de confidentialité suivants: confidentialité sélective de champ, confidentialité en mode connexion, confidentialité de flux de données.	UIT-T M.3016.2
justificatif (*credentials*)	Données transférées pour établir l'identité déclarée d'une entité.	UIT-T X.800

Terme	Définition	Référence
analyse cryptographique (*cryptanalysis*)	1) 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). 2) Processus consistant à récupérer le texte en clair d'un message ou la clé de chiffrement sans avoir accès à la clé. 3) Science de la récupération du contenu d'un message sans accéder à la clé physique (ou à la clé électronique dans un système cryptographique électronique).	UIT-T X.800 UIT-T J.170 UIT-T J.93
algorithme cryptographique (*cryptographic algorithm*)	Fonction mathématique qui calcule un résultat à partir d'une ou de plusieurs valeurs d'entrée.	UIT-T H.235
système de chiffrement (*cryptographic system, cryptosystem*)	1) 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. 2) Un système de chiffrement est simplement un algorithme qui peut convertir des données d'entrée en quelque chose de non reconnaissable (chiffrement), et reconvertir ces données non reconnaissables dans leur forme d'origine (déchiffrement). Les techniques de chiffrement RSA sont décrites dans la Rec. UIT-T X.509.	UIT-T X.509 UIT-T Q.815
cryptographie (*cryptography*)	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.	UIT-T X.800
confidentialité des données (*data confidentiality*)	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.	UIT-T X.509
intégrité des données (*data integrity*)	Propriété assurant que des données n'ont pas été modifiées ou détruites de façon non autorisée.	UIT-T X.800
authentification de l'origine des données (*data origin authentication*)	1) Confirmation que la source des données reçues est telle que déclarée. 2) Corroboration de l'identité de l'entité principale qui est responsable d'une unité de données spécifique.	UIT-T X.800 UIT-T X.811
déchiffrement (*decipherment*)	Opération inverse d'un chiffrement réversible.	UIT-T X.800
décriptage (*decryption*)	Voir décriffrement (*decipherment*).	UIT-T X.800
délégation (*delegation*)	Transfert d'un privilège d'une entité détentrice vers une autre entité.	UIT-T X.509
déni de service (*denial of service*)	Impossibilité d'accès à des ressources pour des utilisateurs autorisés ou introduction d'un retard pour le traitement d'opérations critiques.	UIT-T X.800

Terme	Définition	Référence
signature numérique (*digital signature*)	1) Données ajoutées à une unité de données, ou transformation cryptographique (voir cryptographie (*cryptography*)) 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). 2) Transformation cryptographique d'une unité de données qui permet au destinataire de l'unité de données de prouver l'origine et l'intégrité de cette unité de données, qui protège l'émetteur et le destinateur de l'unité de données contre un faux fabriqué par un tiers et qui protège l'émetteur contre un faux fabriqué par le destinataire.	UIT-T X.800 UIT-T X.843
service d'annuaire (*directory service*)	Service pour la recherche et la récupération d'informations à partir d'un catalogue d'objets bien définis, qui peut contenir des informations sur les certificats, numéros de téléphone, conditions d'accès, adresses, etc. Un exemple en est un service d'annuaire conforme à la Rec. UIT-T X.500.	UIT-T X.843
écoutes (indiscrètes) (*eavesdropping*)	Violation de la confidentialité par surveillance de la communication.	UIT-T M.3016.0
chiffrement (*encipherment*)	1) Transformation cryptographique (voir cryptographie (*cryptography*)) de données produisant un cryptogramme. NOTE – Le chiffrement peut être irréversible. Dans ce cas, le déchiffrement correspondant ne peut pas être effectué. 2) 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.	UIT-T X.800 UIT-T H.235
cryptage (*encryption*)	1) Méthode utilisée pour convertir des informations en clair en cryptogramme. 2) Processus de chiffrement des signaux afin d'éviter un accès non autorisé (voir aussi chiffrement (*encipherment*)).	UIT-T J.170 UIT-T J.93
chiffrement de bout en bout (*end-to-end encipherment*)	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.	UIT-T X.800
entité (*entity*)	1) Un être humain, une organisation, une composante de matériel ou un élément de logiciel. 2) Tout élément concret ou abstrait, qui présente un intérêt. Alors que d'une manière générale le terme entité peut être utilisé pour faire référence à toute chose, son utilisation dans le contexte de la modélisation est réservée aux éléments modélisant l'univers du discours.	UIT-T X.842 UIT-T X.902
authentification d'entité (*entity authentication*)	Corroboration de l'identité d'une entité principale, dans le contexte d'une relation de communication. Note – L'identité authentifiée de cette entité principale n'est garantie que lorsque ce service est invoqué. On peut obtenir la garantie de la continuité d'authentification en suivant la description du 5.2.7/X.811.	UIT-T X.811
preuve (*evidence*)	Information qui, par elle-même ou par association avec d'autres informations, peut être utilisée pour résoudre un litige. *Note* – Formes particulières de preuve: signatures numériques, enveloppes sécurisées et jetons de sécurité. Les signatures numériques sont utilisées avec les techniques de clé publique, tandis que les enveloppes sécurisées et les jetons de sécurité sont utilisés avec les techniques de clé privée.	UIT-T X.813

Terme	Définition	Référence
falsification (*forgery*)	Une entité crée de toutes pièces des informations dont elle prétend qu'elles ont été reçues d'une autre entité ou émises à destination d'une autre entité.	UIT-T M.3016.0
fonction de hachage (*hash function*)	Fonction (mathématique) qui fait correspondre les valeurs d'un grand ensemble (potentiellement très grand) de valeurs à une gamme plus réduite de valeurs.	UIT-T X.810
attaque indirecte (*indirect attack*)	Attaque d'un système qui n'est pas fondé sur les déficiences d'un mécanisme de sécurité particulier (par exemple, attaques qui contournent le mécanisme ou qui dépendent de l'utilisation incorrecte du mécanisme par le système).	UIT-T X.814
intégrité (*integrity*)	Caractéristique de données qui n'ont pas été altérées de façon non autorisée. (Voir aussi intégrité des données (*data integrity*).)	UIT-T H.235
service d'intégrité (*integrity service*)	Le service d'intégrité fournit des moyens permettant d'assurer que les données échangées sont correctes en fournissant une protection contre la modification, la suppression, la création (insertion) et la répétition des données échangées. On peut distinguer les types de service d'intégrité suivants: intégrité sélective de champ; intégrité de connexion sans reprise; intégrité de connexion avec reprise.	UIT-T M.3016.2
menaces intentionnelles (*intentional threats*)	Menaces pouvant aller de l'examen fortuit, utilisant des outils de contrôle facilement disponibles, aux attaques sophistiquées, utilisant une connaissance spéciale du système. Une menace intentionnelle qui se concrétise peut être considérée comme une "attaque".	UIT-T X.800
IPCablecom	Projet UIT-T comprenant une architecture et une série de Recommandations permettant la fourniture de services en temps réel sur les réseaux de télévision par câble utilisant des câblo-modems.	UIT-T J.160
Kerberos	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.	UIT-T J.170
clé (key)	1) Série de symboles commandant les opérations de chiffrement et de déchiffrement. 2) Valeur mathématique introduite dans l'algorithme cryptographique choisi.	UIT-T X.800 UIT-T J.170
échange de clés (*key exchange*)	Echange de clés publiques entre entités à utiliser pour le chiffrement des communications entre ces entités.	UIT-T J.170
gestion de clés (*key management*)	Production, stockage, distribution, suppression, archivage et application de clés conformément à une politique de sécurité.	UIT-T X.800
attaque de l'intercepteur (*man-in-the-middle attack*)	Attaque dans laquelle un attaquant est en mesure de lire, insérer et modifier à volonté des messages entre deux parties sans qu'aucune des parties ne sache que le lien entre elles a été compromis.	UIT-T X.1151
usurpation d'identité (*masquerade*)	Prétention qu'a une entité d'en être une autre.	UIT-T X.800
authentification mutuelle (*mutual authentication*)	Attestation de l'identité des deux entités principales.	UIT-T X.811
non-répudiation (*non-repudiation*)	1) Capacité d'empêcher à un émetteur de nier ultérieurement avoir envoyé un message ou exécuté une action. 2) Protection contre le déni, par une des entités impliquées dans une communication, d'avoir participé à tout ou partie de celle-ci. 3) Processus par lequel l'expéditeur d'un message (par exemple une demande de paiement à la séance) ne peut pas nier avoir envoyé ce message.	UIT-T J.170 UIT-T H.235 UIT-T J.93

Terme	Définition	Référence
notarisation (*notarization*)	Enregistrement de données chez un tiers de confiance permettant de s'assurer ultérieurement de leur exactitude (contenu, origine, date, remise).	UIT-T X.800
menace passive (*passive threat*)	Menace d'une divulgation non autorisée des informations, sans que l'état du système ne soit modifié.	UIT-T X.800
mot de passe (*password*)	1) Information d'authentification confidentielle, habituellement composée d'une chaîne de caractères. 2) Chaîne de mot de passe saisie par l'utilisateur: il s'agit de la clé de sécurité attribuée que l'utilisateur mobile partage avec son domaine de rattachement. Ce mot de passe de l'utilisateur et le secret partagé de l'utilisateur qui en découle doivent être utilisés aux fins d'authentification de l'utilisateur.	UIT-T X.800 UIT-T H.530
sécurité physique (*physical security*)	Mesures prises pour assurer la protection des ressources contre des menaces délibérées ou accidentelles.	UIT-T X.800
entité principale (*principal*)	Entité dont l'identité peut être authentifiée.	UIT-T X.811
respect de la vie privée, secret des communications (*privacy*)	1) 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. 2) 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.	UIT-T X.800 UIT-T H.235
clé privée (*private key*)	1) (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. 2) Clé qui est utilisée avec un algorithme asymétrique de cryptographie et dont la possession est limitée (habituellement à une seule entité). 3) Clé utilisée en cryptographie à clé publique qui appartient à une entité individuelle et qui doit être tenue secrète.	UIT-T X.509 UIT-T X.810 UIT-T J.170
privilège (*privilege*)	Attribut ou propriété attribué par une autorité à un utilisateur.	UIT-T X.509
infrastructure de gestion de privilège (PMI, *privilege management infrastructure*)	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.	UIT-T X.509
clé publique (*public key*)	1) (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. 2) Clé qui est utilisée avec un algorithme asymétrique de cryptographie et qui peut être rendue publique. 3) 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.	UIT-T X.509 UIT-T X.810 UIT-T J.170

Terme	Définition	Référence
certificat de clé publique (*public key certificate*)	1) 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. 2) 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. 3) Relation entre la clé publique d'une entité et un ou plusieurs attributs relatifs à son identité, également appelé certificat numérique.	UIT-T X.509 UIT-T H.235 UIT-T J.170
cryptographie à clé publique (*public key cryptography*)	Technique cryptographique fondée sur un algorithme à deux clés (publique et privée), dans laquelle un message est chiffré avec la clé publique mais ne peut être déchiffré qu'au moyen de la clé privée. Egalement appelé système PPK (clé privée-publique). Note – Le fait de connaître la clé publique ne permet pas d'en déduire la clé privée. Par exemple, le correspondant A construit une clé publique et une clé privée de ce type. Il envoie la clé publique sans restriction à tous ceux qui souhaitent communiquer avec lui, mais il garde la clé privée secrète. Tous ceux qui possèdent la clé publique peuvent alors crypter un message pour le correspondant A, mais seul celui-ci peut décrypter ces messages, à l'aide de sa clé privée.	UIT-T J.93
infrastructure de clé publique (PKI, *public key infrastructure*)	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.	UIT-T X.509
partie utilisatrice (*relying party*)	Utilisateur ou agent qui utilise les données contenues dans un certificat pour prendre des décisions.	UIT-T X.509
répétition (*replay*)	Un message ou une partie d'un message est répété pour produire un effet non autorisé. Par exemple, un message valide contenant des informations d'authentification peut être répété par une autre entité pour s'authentifier elle-même (comme quelque chose qu'elle n'est pas).	UIT-T X.800
répudiation (*repudiation*)	1) Le fait, pour une des entités impliquées dans la communication, de nier avoir participé aux échanges, totalement ou en partie. 2) Une entité nie son implication dans un échange de communication antérieur. 3) (Dans un système MHS, c'est) quand un utilisateur du système MTS ou le système MTS ont ultérieurement la possibilité de refuser le dépôt, la réception ou l'expédition d'un message. Les risques de répudiation sont les suivants: refus d'origine, refus de dépôt, refus de remise.	UIT-T X.800 UIT-T M.3016.0 UIT-T X.402
certificat de révocation de liste (*revocation list certificate*)	Certificat de sécurité qui identifie une liste de certificats de sécurité qui ont été révoqués.	UIT-T X.810
clé secrète (*secret key*)	Clé qui est utilisée avec un algorithme symétrique de cryptographie. La possession de cette clé est limitée (habituellement à deux entités).	UIT-T X.810
sécurité (*security*)	Le terme "sécurité" est utilisé dans le sens d'une minimisation des vulnérabilités d'actifs et de ressources. Un actif est tout élément de valeur. Une vulnérabilité est toute faiblesse qui pourrait être exploitée pour violer un système ou les informations qu'il contient. Une menace est une violation potentielle de la sécurité.	UIT-T X.800
alarme de sécurité (*security alarm*)	Message généré lorsqu'un événement lié à la sécurité, défini par la politique de sécurité comme étant une condition d'alarme, a été détecté. Une alarme de sécurité est destinée à être portée à temps à l'attention d'entités appropriées.	UIT-T X.816

Terme	Définition	Référence
audit de sécurité (*security audit*)	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.	UIT-T X.800
journal d'audit de sécurité (*security audit trail*)	Données collectées et pouvant éventuellement être utilisées pour permettre un audit de sécurité.	UIT-T X.800
certificat de sécurité (*security certificate*)	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. Le terme *certificat de sécurité* est adopté dans la série UIT-T X.800 afin d'éviter des conflits de terminologie avec la Rec. UIT-T X.509.	UIT-T X.810
domaine de sécurité (*security domain*)	1) Ensemble d'utilisateurs et de systèmes faisant l'objet de l'application d'une politique de sécurité commune. 2) Ensemble de ressources associé à une politique de sécurité unique.	UIT-T X.841 UIT-T X.411
information de sécurité (SI, *security information*)	Information nécessaire pour implémenter des services de sécurité.	UIT-T X.810
gestion de la sécurité (*security management*)	La gestion de la sécurité englobe toutes les activités d'établissement, de maintien et de terminaison de caractéristiques de sécurité d'un système. Les sujets suivants sont traités: gestion de services de sécurité; installation de mécanismes de sécurité; gestion des clés (partie de gestion); établissement d'informations d'identité, de clés, de contrôle d'accès, etc.; gestion de la trace de l'audit de sécurité et des alarmes de sécurité.	UIT-T M.3016.0
modèle de sécurité (*security model*)	Cadre pour décrire les services de sécurité destinés à faire face aux éventuelles menaces visant le système MTS et les éléments de sécurité qui sont à la base de ces services.	UIT-T X.402
politique de sécurité (*security policy*)	1) Ensemble de règles fixées par l'autorité de sécurité qui régit l'utilisation et la fourniture de services et de fonctionnalités de sécurité. 2) Ensemble des critères permettant de fournir des services de sécurité. *Note* – 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*). Une politique de sécurité complète traite nécessairement de sujets qui ne relèvent pas du champ d'application de l'OSI.	UIT-T X.509 UIT-T X.800
service de sécurité (*security service*)	Service, fourni par une couche de systèmes ouverts, garantissant une sécurité des systèmes et du transfert de données.	UIT-T X.800
menace de sécurité (menace) (*security threat (threat)*)	Violation potentielle de la sécurité	UIT-T X.800
jeton de sécurité (*security token*)	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.	UIT-T X.810
sensibilité (*sensitivity*)	Caractéristique d'une ressource liée à sa valeur ou à son importance.	UIT-T X.509
secret partagé (*shared secret*)	Clé de sécurité pour les algorithmes cryptographiques; le secret partagé peut être déduit d'un mot de passe.	UIT-T H.530

Terme	Définition	Référence
signature	Voir signature numérique (*digital signature*).	UIT-T X.800
authentification simple (*simple authentication*)	Authentification utilisant de simples accords de mot de passe.	UIT-T X.509
source d'autorité (SOA, *source of authority*)	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.	UIT-T X.509
spam	Courrier électronique non sollicité et non souhaité	UIT-T H.235
usurpation d'identité (*spoofing*)	Usurpation de l'identité d'une ressource ou d'un utilisateur légitime	UIT-T X.509
authentification forte (*strong authentication*)	Authentification utilisant des justificatifs obtenus par des moyens de chiffrement.	UIT-T X.811
attaque Sybil	Attaque visant à corrompre le système de réputation d'un réseau entre homologues en créant un grand nombre d'entités pseudonymes et en les utilisant pour gagner une grande influence, totalement disproportionnée.	
menace (*threat*)	Violation potentielle de la sécurité.	UIT-T X.800
jeton	Voir jeton de sécurité (*security token*)	
cheval de Troie (*Trojan horse*)	Un "cheval de Troie" est un programme introduit dans le système avec une fonction non autorisée, en plus de sa fonction autorisée. Un relais qui copie également des messages à destination d'une voie non autorisée est un "cheval de Troie".	UIT-T X.800
confiance (*trust*)	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.	UIT-T X.810
fonctionnalité de confiance (*trusted functionality*)	Fonctionnalité perçue comme correcte en ce qui concerne certains critères, tels que ceux qui sont définis par une politique de sécurité, par exemple.	UIT-T X.800
tierce partie de confiance (TTP, *trusted third party*)	Autorité de sécurité ou son agent auquel d'autres entités font confiance au regard de certaines activités liées à la sécurité (dans le contexte d'une politique de sécurité).	UIT-T X.810
réseau de capteurs ubiquitaires (USN, *ubiquitous sensor network*)	Réseau qui utilise des capteurs à faible coût et à faible puissance pour développer la perception du contexte afin de communiquer des données captées à toute personne, où qu'elle se trouve et à tout moment. Un réseau USN peut couvrir une grande zone géographique et peut prendre en charge diverses applications.	
accès non autorisé (*unauthorized access*)	Une entité tente d'accéder à des données en violation de la politique de sécurité en vigueur.	UIT-T M.3016.0
authentification de l'utilisateur (*user authentication*)	Fourniture de la preuve de l'identité d'un utilisateur humain ou d'un processus d'application.	UIT-T M.3016.0
vérificateur (*verifier*)	Entité qui est ou qui représente l'entité revendiquant une identité authentifiée. Un vérificateur comporte les fonctions nécessaires pour engager des échanges pour authentification.	UIT-T X.811
vulnérabilité (*vulnerability*)	Toute faiblesse qui pourrait être exploitée pour violer un système ou les informations qu'il contient.	UIT-T X.800

Terme	Définition	Référence
certificat UIT-T X.509 (*ITU-T X.509 certificate*)	Spécification de certificat de clé publique élaborée dans le cadre de la norme d'annuaire UIT-T X.500.	UIT-T J.170

Annexe B

Acronymes et abréviations

Annexe B

Acronymes et abréviations

Acronyme	Signification
ACI	information de contrôle d'accès (*access control information*)
AES	norme de chiffrement perfectionné (*advanced encryption standard algorithm*)
ASN.1	notation de syntaxe abstraite numéro un (*abstract syntax notation one*)
ASP	fournisseur de service d'application (*application service provider*)
ATIS	Alliance for Telecommunications Industry Solutions
A/V	audiovisuel
BioAPI	interface de programmation d'application biométrique (*biometric application program/programming interface*)
BPON	réseau optique passif à large bande (*broadband passive optical network*)
B2C	entreprise-client (*business-to-customer*)
CA	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, délivre les certificats et tient à jour les informations d'état concernant les certificats.
CASF	fonctions antispam centrales (*core anti-spam functions*)
CIRT	équipe d'intervention en cas d'incident informatique (*computer incident response team*)
CDMA	accès multiple par répartition en code (*code division multiple access*)
CMIP	protocole commun d'informations de gestion (*common management information protocol*)
CORBA	architecture de courtier commun de requêtes d'objets (*common object request broker architecture*)
CP	politique de certificat (*certificate policy*)
CPS	déclaration de pratique de certification (*certification practice statement*)
CRL	liste de révocation de certificats (*certificate revocation list*)
CVE	vulnérabilités et expositions courantes (*common vulnerabilities and exposures*)
CVSS	système d'évaluation des vulnérabilités courantes (*common vulnerability scoring system*)
CYBEX	échange d'informations de cybersécurité (*cybersecurity information exchange*)
DNS	serveur/système/service de noms de domaine (*domain name server/system/service*)
DSL	boucle d'abonné numérique (*digital subscriber loop*)
EAP	protocole d'authentification extensible (*extensible authentication protocol*)
ENISA	Agence européenne chargée de la sécurité des réseaux et de l'information (*European Network and Information Security Agency*)
ETSI	Institut européen des normes de télécommunication (*European Telecommunications Standards Institute*)
FMC	convergence fixe-mobile (*fixed mobile convergence*)
FW	pare-feu (*firewall*)
GK	portier (*gatekeeper*)

Acronyme	Signification
GPRS	système général de radiocommunications par paquets (*general packet radio system*)
GSM	système mondial de communications mobiles (*global system for mobile communications*)
GW	passerelle (*gateway*)
HFX	chiffrement de télécopie de Hawthorne (*Hawthorne facsimile cipher*)
HKM	algorithme de gestion de clés de Hawthorne (*Hawthorne key management algorithm*)
HTTP	protocole de transfert hypertexte (*hypertext transfer protocol*)
TIC	technologies de l'information et de la communication
ID	identificateur
IdM	gestion d'identité (*identity management*)
CEI	Commission électrotechnique internationale
IEEE	Institut des ingénieurs en électricité et en électronique (*Institute of Electrical and Electronics Engineers*)
IETF	Groupe d'étude sur l'ingénierie Internet (*Internet Engineering Task Force*)
IKE	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.
IM	messagerie instantanée (*instant messaging*)
IMS	sous-système multimédia IP (*IP multimedia subsystem*)
IMT-2000	télécommunications mobiles internationales 2000 (*international mobile telecommunications 2000*)
IP	protocole Internet (*Internet protocol*)
IPSec	sécurité du protocole Internet (*Internet protocol security*)
TVIP	télévision utilisant le protocole Internet
ISMF	cadre de gestion de la sécurité de l'information (*information security management framework*)
IPX	échange de paquets Internet (*Internet packet exchange*)
ISMS	système de gestion de la sécurité de l'information (*information security management system*)
ISO	Organisation internationale de normalisation (*International Organization for Standardization*)
UIT-T	Secteur de la normalisation des télécommunications de l'Union internationale des télécommunications
LAN	réseau local (*local area network*)
LDAP	protocole rapide d'accès à l'annuaire (*lightweight directory access protocol*)
MD5	condensé de message N° 5 (*message digest No. 5*) (algorithme de hachage sécurisé)
MIS	système d'informations de gestion (*management information system*)
MMS	service de messagerie multimédia (*multimedia messaging service*)
MTA	agent de transfert de messages (*message transfer agent*) (dans les systèmes de messagerie) adaptateur de terminal média (*media terminal adapter*) (dans les systèmes de transmission par câble)
MWSSG	passerelle de sécurité pour les services web mobiles (*mobile web services security gateway*)
NAT	traduction d'adresse réseau (*network address translation*)

Acronyme	Signification
NGN	réseau de prochaine génération (*next generation network*)
OASIS	Organisation pour le progrès des normes sur les informations structurées (*Organization for the Advancement of Structured Information Standards*)
OMG	groupe de gestion d'objets (*Object Management Group*)
OSI	interconnexion des systèmes ouverts (*open systems interconnection*)
P2P	homologue à homologue (*peer-to-peer*)
PC	ordinateur personnel (*personal computer*)
PDA	assistant personnel électronique (*personal data assistant*)
PIN	numéro d'identification personnel (*personal identification number*)
PII	information d'identification personnelle (*personally identifiable information*)
PKI	infrastructure de clé publique (*public-key infrastructure*)
PKINIT	authentification initiale par cryptographie à clé publique (*public-key cryptography initial authentication*)
PMI	infrastructure de gestion de privilège (*privilege management infrastructure*)
PSS	service de protection des informations PII (*PII protection service*)
RTPC	réseau téléphonique public commuté
QoS	qualité de service (*quality of service*)
RASF	fonctions antispam côté destinataire (*recipient-side anti-spam functions*)
RBAC	contrôle d'accès basé sur le rôle (*role-based access control*)
RBL	listes de blocage en temps réel (*real-time blocking list*)
RFID	identification par radiofréquence (*radio frequency identification*)
RSA	Rivest, Shamir et Adleman (algorithme à clé publique)
RTP	protocole de transport en temps réel (*real time protocol*)
SAML	langage de balisage d'assertion de sécurité (*security assertion mark-up language*)
SASF	fonctions antispam côté expéditeur (*sender-side anti-spam functions*)
CE	Commission d'études
SHA1	algorithme de hachage sécurisé numéro un (*secure hash algorithm 1*)
SIP	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.
SMS	service de messages courts (*short message service*)
SMTP	protocole simple de transfert de courrier (*simple mail transfer protocol*)
SNMP	protocole simple de gestion de réseau (*simple network management protocol*)
SoA	source d'autorité (*source of authority*)
SOA	architecture orientée service (*service oriented architecture*)
SPAK	protocole d'authentification sûre par mot de passe avec échange de clés (*secure password-based authentication protocol with key exchange*)
SSL	couche de connecteurs sécurisés (*secure socket layer*)

Acronyme	Signification
SSO	connexion unique (*single sign-on*)
TCP/IP	protocole de commande de transmission/protocole Internet (*transmission control protocol/internet protocol*)
TNSS	système de sécurité d'un réseau de télécommunication IP (*telecommunication IP-based network security system*)
TLS	sécurité de la couche transport (*transport layer security*)
RGT	réseau de gestion des télécommunications
UE	équipement d'utilisateur (*user equipment*)
UICC	carte de circuit intégré universelle (*universal integrated circuit card*)
URS	système de réputation des utilisateurs (*user reputation system*)
USN	réseau de capteurs ubiquitaires (*ubiquitous sensor network*)
VoIP	téléphonie IP, voix sur IP (*voice over IP*)
VPN	réseau privé virtuel (*virtual private network*)
VSPPS	serveur de politique de prévention des spams de VoIP (*VoIP spam prevention policy server*)
VSPS	système de prévention des spams de VoIP (*VoIP spam prevention system*)
WAN	réseau étendu (*wide area network*)
Wi-Fi	fidélité sans fil (*wireless fidelity*) (marque déposée de l'Alliance Wi-Fi pour les produits certifiés basés sur les normes IEEE 802.11)
AMNT	Assemblée mondiale de normalisation des télécommunications
XACML	langage de balisage extensible de contrôle d'accès (*extensible access control mark-up language*)
XML	langage de balisage extensible (*extensible mark-up language*)
3G	troisième génération (*3rd generation*)
3GPP	projet de partenariat de troisième génération (*3rd generation partnership project*)
3GPP2	projet de partenariat de troisième génération numéro deux (*3rd generation partnership project 2*)

Annexe C

Présentation succincte des Commissions d'études de l'UIT-T menant des activités dans le domaine de la sécurité

Annexe C

Présentation succincte des Commissions d'études de l'UIT-T menant des activités dans le domaine de la sécurité

La plupart des Commissions d'études étudient au moins certains aspects de la sécurité des télécommunications et/ou des TIC. La Commission d'études 17, dont le domaine d'étude général est la sécurité, a été désignée Commission d'études directrice pour la sécurité et chacune des autres Commissions d'études est chargée d'étudier les questions de sécurité qui relèvent de son propre domaine de compétence. Le Tableau 9 répertorie les Commissions d'études ayant des responsabilités dans le domaine de la sécurité et énumère les rôles qu'elles ont en tant que Commission d'études directrice pendant la période d'études 2009-2012.

Tableau 9 – Commissions d'études ayant des responsabilités dans le domaine de la sécurité

Commission d'études	Titre	Responsabilités/rôle dans le domaine de la sécurité
CE 2	Aspects opérationnels de la fourniture de services et de la gestion des télécommunications	Commission d'études directrice pour la définition des services, le numérotage et le routage Commission d'études directrice pour les télécommunications utilisées pour les secours en cas de catastrophe/l'alerte avancée Commission d'études directrice pour la gestion des télécommunications
CE 5	Environnement et changement climatique	Commission d'études directrice pour la compatibilité électromagnétique et les effets électromagnétiques Commission d'études directrice pour les TIC et le changement climatique
CE 9	Transmission télévisuelle et sonore et réseaux câblés intégrés à large bande	Commission d'études directrice pour les réseaux de télévision et câblés intégrés large bande
CE 11	Spécifications de signalisation, protocoles et spécifications de test	Commission d'études directrice pour la signalisation et les protocoles Commission d'études directrice pour les réseaux intelligents Commission d'études directrice pour les spécifications de test
CE 12	Qualité de fonctionnement, qualité de service et qualité d'expérience	Commission d'études directrice pour la qualité de service et la qualité d'expérience
CE 13	Réseaux futurs, y compris les réseaux mobiles et les réseaux de prochaine génération	Commission d'études directrice pour les réseaux futurs et les NGN Commission d'études directrice pour la gestion de la mobilité et la convergence fixe-mobile
CE 15	Infrastructures des réseaux de transport optiques et des réseaux d'accès	Commission d'études directrice pour le transport dans le réseau d'accès Commission d'études directrice pour les technologies optiques Commission d'études directrice pour les réseaux de transport optiques

Commission d'études	Titre	Responsabilités/rôle dans le domaine de la sécurité
CE 16	Codage, systèmes et applications multimédias	Commission d'études directrice pour le codage, les systèmes et les applications multimédias Commission d'études directrice pour les applications ubiquitaires ("tout en ligne", par exemple la cybersanté) Commission d'études directrice pour l'accessibilité des télécommunications/TIC pour les personnes handicapées
CE 17	Sécurité	Commission d'études directrice pour la sécurité des télécommunications Commission d'études directrice pour la gestion d'identité Commission d'études directrice pour les langages et les techniques de description

Annexe D

Recommandations et autres publications sur la sécurité mentionnées dans le présent Manuel

Annexe D

Recommandations et autres publications sur la sécurité mentionnées dans le présent Manuel

La présente Annexe contient une liste complète de toutes les Recommandations UIT-T mentionnées dans le présent Manuel avec des hyperliens, ce qui permet, à partir de la version électronique du texte, d'accéder directement aux Recommandations et de les télécharger. Comme indiqué dans le texte, l'UIT-T a élaboré de nombreuses normes relatives à la sécurité en collaboration avec d'autres organisations de normalisation. Les Recommandations en vigueur relatives à la sécurité des TIC dont le texte a été établi en commun avec une autre organisation sont également incluses dans ce tableau. L'ensemble complet des Recommandations UIT-T est accessible en ligne à l'adresse suivante: http://www.itu.int/en/ITU-T/publications/Pages/recs.aspx. Les Recommandations UIT-T relatives à la sécurité sont disponibles via la Partie 2 (base de données) de la feuille de route sur les normes de sécurité (www.itu.int/ITU-T/studygroups/com17/ict/index.html).

Recommandation	Titre	Texte équivalent
UIT-T E.408	Prescriptions de sécurité des réseaux de télécommunication	
UIT-T E.409	Organisation en cas d'incident et prise en charge des incidents relatifs à la sécurité: lignes directrices destinées aux organisations de télécommunication	
UIT-T F.744	Description et spécifications de service concernant les intergiciels des réseaux de capteurs ubiquitaires	
UIT-T G.827	Paramètres et objectifs de disponibilité pour les conduits numériques internationaux de bout en bout à débit constant	
UIT-T G.1000	Qualité de service des communications: cadre et définitions	
UIT-T G.1030	Evaluation de la qualité de fonctionnement de bout en bout dans les réseaux IP pour les applications de transmission de données	
UIT-T G.1050	Modèle de réseau pour l'évaluation de la qualité de transmission multimédia sur protocole Internet	
UIT-T G.1081	Points de surveillance de la qualité de fonctionnement pour la TVIP	
UIT-T H.235.0	Cadre de sécurité H.323: cadre de sécurité pour les systèmes multimédias de la série H (systèmes H.323 et autres systèmes de type H.245)	
UIT-T H.235.1	Cadre de sécurité H.323: profil de sécurité de base	
UIT-T H.235.2	Cadre de sécurité H.323: profil de sécurité avec signature	
UIT-T H.235.3	Cadre de sécurité H.323: profil de sécurité hybride	
UIT-T H.235.4	Cadre de sécurité H.323: sécurité des appels à routage direct et des appels à routage sélectif	
UIT-T H.235.5	Cadre de sécurité H.323: cadre de l'authentification sécurisée pendant l'échange de messages RAS au moyen de secrets partagés faibles	
UIT-T H.235.6	Cadre de sécurité H.323: profil pour le chiffrement vocal avec gestion de clés native dans les systèmes H.235/H.245	
Guide de mise en oeuvre UIT-T H.235	Guide de mise en œuvre de la version 3 de la Recommandation UIT-T H.235: Sécurité et chiffrement pour les terminaux multimédias de la série H (terminaux UIT-T H.323 et autres terminaux de type UIT-T H.245)	
UIT-T H.323	Systèmes de communication multimédia en mode paquet	

Recommandation	Titre	Texte équivalent
UIT-T H.350	Architecture des services d'annuaire pour les conférences multimédias	
UIT-T H.460.17	Utilisation de la connexion de signalisation d'appel H.225.0 pour le transport de messages RAS H.323	
UIT-T H.460.18	Traversée de traducteurs d'adresse de réseau et de pare-feu par des flux de signalisation H.323	
UIT-T H.460.19	Traversée de traducteurs d'adresse de réseau et de pare-feu par des flux de média H.323	
UIT-T H.510	Mobilité pour systèmes et services multimédias H.323	
UIT-T H.530	Procédures de sécurité symétrique pour la mobilité des systèmes H.323 selon la Recommandation H.510	
UIT-T J.160	Cadre architectural pour l'acheminement de services à temps critique sur les réseaux de télévision par câble utilisant des câblo-modems	
UIT-T J.170	Spécification de la sécurité sur IPCablecom	
UIT-T J.360	Architecture générale IPCablecom2	
UIT-T M.3010	Principes du réseau de gestion des télécommunications	
UIT-T M.3016.0	Sécurité pour le plan de gestion: aperçu général	
UIT-T M.3016.1	Sécurité pour le plan de gestion: prescriptions de sécurité	
UIT-T M.3016.2	Sécurité pour le plan de gestion: services de sécurité	
UIT-T M.3016.3	Sécurité pour le plan de gestion: mécanisme de sécurité	
UIT-T M.3016.4	Sécurité pour le plan de gestion: Formulaire des profils de sécurité	
UIT-T M.3208.2	Services de gestion RGT pour réseaux à circuits spécialisés et circuits reconfigurables: gestion des connexions de liaison de service préapprovisionnées pour la formation d'un service de circuit loué	
UIT-T M.3210.1	Services de gestion RGT pour la gestion de la sécurité des réseaux IMT-2000	
UIT-T Q.816	Services RGT à architecture CORBA	
UIT-T Q.834.3	Description en langage UML des prescriptions relatives aux interfaces de gestion des réseaux optiques passifs à large bande	
UIT-T Q.834.4	Spécification d'une interface en architecture CORBA pour les réseaux optiques passifs à large bande basée sur les prescriptions d'interface UML	
UIT-T Q.1701	Cadre général des réseaux IMT-2000	
UIT-T Q.1702	Aspects réseau au-delà des systèmes IMT-2000 – Vision à long terme	
UIT-T Q.1703	Cadre général des capacités de service et de réseau des aspects réseau des systèmes au-delà de l'IMT-2000	
UIT-T 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)	Recense des documents du 3GPP
UIT-T Q.1742.1	Références IMT-2000 au réseau central évolué ANSI-41 avec réseau d'accès cdma2000	Recense des documents du 3GPP2
UIT-T T.4	Normalisation des télécopieurs du Groupe 3 pour la transmission de documents	
UIT-T T.36	Capacités de sécurité à utiliser avec les télécopieurs du Groupe 3	
UIT-T T.37	Procédures pour le transfert de données de télécopie en mode différé sur le réseau Internet	

Recommandation	Titre	Texte équivalent
UIT-T T.38	Procédures de communication de télécopie du Groupe 3 en temps réel sur les réseaux à protocole Internet	
UIT-T T.563	Caractéristiques des télécopieurs du Groupe 4	
UIT-T X.500	L'annuaire: aperçu général des concepts, modèles et services	ISO/CEI 9594-1
UIT-T X.501	L'annuaire: les modèles	ISO/CEI 9594-2
UIT-T X.509	L'annuaire: cadre général des certificats de clé publique et d'attribut	ISO/CEI 9594-8
UIT-T X.511	L'annuaire: définition du service abstrait	ISO/CEI 9594-3
UIT-T X.518	L'annuaire: procédures pour le fonctionnement réparti	ISO/CEI 9594-4
UIT-T X.519	L'annuaire: spécification des protocoles	ISO/CEI 9594-5
UIT-T X.520	L'annuaire: types d'attributs sélectionnés	ISO/CEI 9594-6
UIT-T X.521	L'annuaire: classes d'objets sélectionnées	ISO/CEI 9594-7
UIT-T X.525	L'annuaire: duplication	ISO/CEI 9594-9
UIT-T X.530	L'annuaire: utilisation de la gestion-systèmes pour l'administration de l'annuaire	ISO/CEI 9594-10
UIT-T X.711	Protocole commun d'information de gestion: spécification	ISO/CEI 9596-1
UIT-T X.736	Gestion-systèmes: fonction de signalisation des alarmes de sécurité	ISO/CEI 10164-7
UIT-T X.740	Gestion-systèmes: fonction de piste de vérification de sécurité	ISO/CEI 10164-8
UIT-T X.741	Gestion-systèmes: objets et attributs de contrôle d'accès	ISO/CEI 10164-9
UIT-T X.780	Directives concernant le RGT pour la définition d'objets gérés CORBA	
UIT-T X.780.1	Directives concernant le RGT pour la définition d'interfaces d'objets gérés CORBA à granularité grossière	
UIT-T X.780.2	Lignes directrices relatives au RGT pour la définition d'objets gérés et d'objets de façade CORBA orientés service	
UIT-T X.781	Spécifications et directives pour l'établissement de formulaires de déclaration de conformité d'implémentations associés aux systèmes de type CORBA	
UIT-T X.790	Fonction de gestion des dérangements pour les applications de l'UIT-T	
UIT-T X.800	Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT	ISO/CEI 7498-2
UIT-T X.802	Modèle de sécurité des couches inférieures	ISO/CEI TR 13594
UIT-T X.803	Modèle de sécurité pour les couches supérieures	ISO/CEI 10745
UIT-T X.805	Architecture de sécurité pour les systèmes assurant des communications de bout en bout	ISO/CEI 18028-2
UIT-T X.810	Cadres de sécurité pour les systèmes ouverts: aperçu général	ISO/CEI 10181-1
UIT-T X.811	Cadres de sécurité pour les systèmes ouverts: cadre d'authentification	ISO/CEI 10181-2
UIT-T X.812	Cadres de sécurité pour les systèmes ouverts: cadre de contrôle d'accès	ISO/CEI 10181-3
UIT-T X.813	Cadres de sécurité pour les systèmes ouverts: non-répudiation	ISO/CEI 10181-4
UIT-T X.814	Cadres de sécurité pour les systèmes ouverts: cadre de confidentialité	ISO/CEI 10181-5
UIT-T X.815	Cadres de sécurité pour les systèmes ouverts: cadre d'intégrité	ISO/CEI 10181-6
UIT-T X.816	Cadres de sécurité pour les systèmes ouverts: cadre d'audit et d'alarmes de sécurité	ISO/CEI 10181-7
UIT-T X.830	Sécurité générique des couches supérieures: aperçu général, modèles et notation	ISO/CEI 11586-1

Recommandation	Titre	Texte équivalent
UIT-T X.831	Sécurité générique des couches supérieures: définition du service assuré par l'élément de service d'échange de sécurité	ISO/CEI 11586-2
UIT-T X.832	Sécurité générique des couches supérieures: spécification du protocole d'élément de service d'échange de sécurité	ISO/CEI 11586-3
UIT-T X.833	Sécurité générique des couches supérieures: spécification de la syntaxe de protection du transfert	ISO/CEI 11586-4
UIT-T X.834	Sécurité générique des couches supérieures: formulaire PICS de l'élément de service d'échange de sécurité (SESE)	ISO/CEI 11586-5
UIT-T X.835	Sécurité générique des couches supérieures: formulaire PICS de la syntaxe de protection de transfert	ISO/CEI 11586-6
UIT-T X.841	Techniques de sécurité – Objets informationnels de sécurité pour le contrôle d'accès	ISO/CEI 15816
UIT-T X.842	Techniques de sécurité – Lignes directrices pour l'utilisation et la gestion des services de tiers de confiance	ISO/CEI TR 14516
UIT-T X.843	Techniques de sécurité – Spécification de services de tiers de confiance pour la prise en charge des applications de signature numérique	ISO/CEI 15945
UIT-T X.1031	Rôle des utilisateurs finals et des réseaux de télécommunication dans l'architecture de sécurité	
UIT-T X.1032	Architecture de corrélations externes dans un système de sécurité d'un réseau de télécommunication IP	
UIT-T X.1034	Lignes directrices sur l'authentification et la gestion de clé basées sur le protocole d'authentification extensible dans un réseau de communication de données	
UIT-T X.1035	Protocole d'échange de clés avec authentification par mot de passe	
UIT-T X.1036	Cadre applicable à la création, au stockage, à la distribution et à la mise en vigueur des politiques de sécurité de réseau	
UIT-T X.1051	Techniques de sécurité – Lignes directrices basées sur la norme ISO/CEI 27002 pour la gestion de la sécurité des informations pour les organisations de télécommunication	ISO/CEI 27011
UIT-T X.1052	Cadre de gestion de la sécurité de l'information	
UIT-T X.1055	Guide concernant la gestion des risques et les profils de risques pour les organisations de télécommunication	
UIT-T X.1056	Lignes directrices relatives à la gestion des incidents de sécurité pour les organisations de télécommunication	
UIT-T X.1057	Lignes directrices relatives à la gestion des actifs dans les organisations de télécommunication	
UIT-T X.1081	Cadre général pour la spécification des aspects de sécurité et d'innocuité de la télébiométrie	
UIT-T X.1080.1	Cybersanté et systèmes mondiaux de télémédecine - Protocole générique de télécommunication	
UIT-T X.1082	Télébiométrie relative à la physiologie humaine	ISO/CEI 80000-14
UIT-T X.1083	Biométrie – Protocole d'interfonctionnement à l'interface BioAPI	ISO/CEI 24708
UIT-T X.1084	Mécanisme de système télébiométrique – Partie 1: Protocole général d'authentification biométrique et profils types pour les systèmes de télécommunication	
UIT-T X.1086	Procédures de protection télébiométriques – Lignes directrices relatives aux mesures techniques et de gestion pour la sécurité des données biométriques	
UIT-T X.1088	Cadre général des clés numériques télébiométriques – Cadre pour la génération et la protection des clés numériques biométriques	

Recommandation	Titre	Texte équivalent
UIT-T X.1089	Infrastructure d'authentification télébiométrique	
UIT-T X.1090	Cadre d'authentification avec gabarit télébiométrique à usage unique	
UIT-T X.1101	Exigences de sécurité et cadre applicables aux communications en multidiffusion	
UIT-T X.1111	Cadre général des technologies de sécurité pour les réseaux domestiques	
UIT-T X.1112	Profil de certificat pour les dispositifs présents dans le réseau domestique	
UIT-T X.1113	Lignes directrices applicables aux mécanismes d'authentification de l'utilisateur pour les services assurés dans le réseau domestique	
UIT-T X.1114	Cadre d'autorisation pour le réseau domestique	
UIT-T X.1121	Cadre général des technologies de la sécurité pour les communications mobiles de données de bout en bout	
UIT-T X.1122	Lignes directrices pour la réalisation de systèmes mobiles sécurisés basés sur l'infrastructure de clés publiques (PKI)	
UIT-T X.1123	Service de sécurité différencié pour les communications mobiles sécurisées de données de bout en bout	
UIT-T X.1124	Architecture d'authentification pour les communications de données de bout en bout dans les réseaux mobiles	
UIT-T X.1125	Système de réaction corrélative pour les communications de données dans les réseaux mobiles	
UIT-T X.1141	Langage de balisage d'assertion de sécurité (SAML 2.0)	OASIS SAML 2.0
UIT-T X.1142	Langage de balisage extensible de contrôle d'accès (XACML 2.0)	OASIS XACML 2.0
UIT-T X.1143	Architecture de sécurité des messages dans l'environnement des services web mobiles	
UIT-T X.1151	Lignes directrices applicables à un protocole d'authentification sûre fondée sur un mot de passe avec échange de clés	
UIT-T X.1152	Techniques de communication de données de bout en bout sécurisée reposant sur des services de tiers de confiance	
UIT-T X.1153	Cadre de gestion d'un service d'authentification reposant sur un mot de passe à usage unique	
UIT-T X.1161	Cadre général des communications sécurisées entre homologues	
UIT-T X.1162	Architecture de sécurité et opérations dans les réseaux entre homologues	
UIT-T X.1171	Menaces et protection requise pour les informations d'identification personnelle dans les applications utilisant l'identification par étiquette	
UIT-T X.1191	Spécifications fonctionnelles et architecture concernant les aspects de sécurité de la TVIP	
UIT-T X.1192	Spécifications fonctionnelles et mécanismes relatifs au transcodage sécurisé pour la TVIP	
UIT-T X.1193	Cadre de gestion des clés pour les services sécurisés de télévision utilisant le protocole Internet	
UIT-T X.1195	Mécanisme d'interopérabilité de la protection de service et de contenu	
UIT-T X.1205	Présentation générale de la cybersécurité	

Recommandation	Titre	Texte équivalent
UIT-T X.1206	Cadre indépendant du fournisseur de produits pour la notification automatique d'informations de sécurité et la diffusion automatique de mises à jour	
UIT-T X.1207	Lignes directrices à l'intention des fournisseurs de services de télécommunication pour lutter contre les risques d'installation de logiciels espions ou de tout logiciel potentiellement indésirable	
UIT-T X.1209	Capacités et scénarios de contexte associés pour le partage et l'échange d'informations sur la cybersécurité	
UIT-T X.1231	Stratégies techniques de lutte contre le spam	
UIT-T X.1240	Technologies intervenant dans la lutte contre le spam par courrier électronique	
UIT-T X.1241	Cadre technique pour lutter contre les spams par courrier électronique	
UIT-T X.1242	Système de filtrage des spams du service de messages courts (SMS) basé sur des règles spécifiées par l'utilisateur	
UIT-T X.1243	Système de passerelle interactive pour lutter contre le spam	
UIT-T X.1244	Aspects généraux de la lutte contre le spam dans les applications multimédias IP	
UIT-T X.1245	Cadre de lutte contre le spam dans les applications multimédias IP	
UIT-T X.1250	Capacités de base pour l'amélioration de l'interopérabilité globale dans la gestion d'identité	
UIT-T X.1251	Cadre de contrôle de l'identité numérique par l'utilisateur	
UIT-T X.1252	Termes et définitions de base relatifs à la gestion d'identité	
UIT-T X.1253	Lignes directrices pour la sécurité des systèmes de gestion d'identité	
UIT-T X.1303	Protocole d'alerte commun (CAP 1.1)	OASIS CAP v1.1
UIT-T X.1311	Cadre de sécurité des réseaux de capteurs ubiquitaires	
UIT-T X.1312	Lignes directrices sur la sécurité des intergiciels des réseaux de capteurs ubiquitaires	
UIT-T X.1500	Techniques d'échange d'informations sur la cybersécurité	
UIT-T X.1520	Vulnérabilités et expositions courantes	
UIT-T X.1521	Système d'évaluation des vulnérabilités courantes	
UIT-T X.1570	Mécanismes de découverte pour l'échange d'informations de cybersécurité	
UIT-T Y.2001	Aperçu général des réseaux de prochaine génération	
UIT-T Y.2701	Prescriptions de sécurité des réseaux de prochaine génération de version 1	
UIT-T Y.2702	Spécifications d'authentification et d'autorisation pour les réseaux de prochaine génération version 1	
UIT-T Y.2703	Application du service d'authentification, d'autorisation et de comptabilité dans les NGN	
UIT-T Y.2704	Mécanismes et procédures de sécurité des réseaux NGN	
UIT-T Y.2720	Cadre de gestion d'identité des réseaux NGN	
UIT-T Y.2721	Spécifications et cas d'utilisation de la gestion d'identité dans les réseaux NGN	
UIT-T Y.2722	Mécanismes de gestion d'identité dans les réseaux de prochaine génération	
UIT-T Y.2740	Spécifications de sécurité applicables aux transactions financières mobiles à distance dans les réseaux de prochaine génération	

Recommandation	Titre	Texte équivalent
UIT-T Y.2741	Architecture de sécurité applicable aux transactions financières sur mobile dans les réseaux de prochaine génération	
UIT-T Y.2760	Cadre de sécurité pour la mobilité dans les réseaux de prochaine génération	

Publication	Titre	Texte équivalent
Suppléments aux Recommandations UIT-T de la série X		
Supplément 3	Série UIT-T X.800-X.849 – Supplément sur les lignes directrices pour la mise en œuvre de la sécurité dans les systèmes et dans les réseaux	
Supplément 6	Série UIT-T X.1240 – Supplément sur la lutte contre le spam et les menaces associées	
Supplément 7	Série UIT-T X.1250 – Supplément relatif à la présentation de la gestion d'identité dans le cadre de la cybersécurité	
Supplément 8	UIT-T X.1205 – Supplément sur les bonnes pratiques de lutte contre les menaces liées aux botnets	
Supplément 9	UIT-T X.1205 – Supplément sur les lignes directrices visant à réduire les maliciels dans les réseaux TIC	
Supplément 10	UIT-T X.1205 – Supplément sur les possibilités d'utilisation du retraçage dans les réseaux	
Supplément 11	UIT-T X.1245 – Supplément sur le cadre de lutte contre le spam de VoIP fondé sur l'utilisation de listes de blocage en temps réel (RBL)	
Manuels UIT-T		
lien	Technologies des installations extérieures appliquées aux réseaux publics	
lien	Application des ordinateurs et des microprocesseurs à la fabrication, à l'installation et à la protection des câbles de télécommunication	

UIT-T – Bureau de la normalisation des télécommunications (TSB)
Place des Nations – CH-1211 Genève 20 – Suisse
E-mail: tsbmail@itu.int Web: www.itu.int/ITU-T

Imprimé en Suisse
Genève, 2012
ISBN 978-92-61-14002-1