UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

CCITT X.800

COMITÉ CONSULTATIF
INTERNATIONAL
TÉLÉGRAPHIQUE ET TÉLÉPHONIQUE

RÉSEAUX DE COMMUNICATIONS DE DONNÉES: INTERCONNEXION DE SYSTÈMES OUVERTS (OSI); SÉCURITÉ, STRUCTURE ET APPLICATIONS

ARCHITECTURE DE SÉCURITÉ POUR L'INTERCONNEXION EN SYSTÈMES OUVERTS D'APPLICATIONS DU CCITT

Recommandation X.800

Genève, 1991

AVANT-PROPOS

Le CCITT (Comité consultatif international télégraphique et téléphonique) est un organe permanent de l'Union internationale des télécommunications (UIT). Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée plénière du CCITT, qui se réunit tous les quatre ans, détermine les thèmes d'études et approuve les Recommandations rédigées par ses Commissions d'études. Entre les Assemblées plénières, l'approbation des Recommandations par les membres du CCITT s'effectue selon la procédure définie dans la Résolution nº 2 du CCITT (Melbourne, 1988).

La Recommandation X.800 que l'on doit à la Commission d'études VII, a été approuvée le 22 mars 1991 selon la procédure définie dans la Résolution nº 2.

NOTE DU CCITT

Dans cette Recommandation, l'expression «Administration» est utilisée pour désigner de façon abrégée aussi bien une Administration de télécommunications qu'une exploitation privée reconnue de télécommunications.

Recommandation X.800

ARCHITECTURE DE SÉCURITÉ POUR L'INTERCONNEXION EN SYSTÈMES OUVERTS D'APPLICATIONS DU CCITT [1)]

0 Introduction

La Recommandation X.200 décrit le modèle de référence pour l'interconnexion des systèmes ouverts (OSI). Elle établit un cadre permettant de coordonner le développement des Recommandations existantes et à venir pour l'interconnexion des systèmes.

L'objectif de l'OSI est de permettre l'interconnexion de systèmes informatiques hétérogènes de façon à réaliser des communications utiles entre des processus d'application. A différents moments, des contrôles de sécurité doivent être établis pour protéger les informations échangées entre les processus d'application. Ces contrôles devraient rendre le coût d'obtention ou de modification incorrecte des données plus important que la valeur potentielle de cette action ou allonger tellement la durée requise pour obtenir incorrectement les données que la valeur de celles-ci serait perdue.

La présente Recommandation définit les éléments généraux d'architecture ayant trait à la sécurité, que l'on peut appliquer de façon appropriée dans les cas où une protection de la communication entre systèmes ouverts est requise. Dans le cadre du modèle de référence, elle établit des principes directeurs et des contraintes permettant d'améliorer les Recommandations existantes ou d'élaborer de nouvelles Recommandations dans le contexte de l'OSI pour permettre des communications sûres et donner ainsi une approche cohérente de la sécurité dans l'OSI.

Des connaissances de base en matière de sécurité aideront à comprendre la présente Recommandation. Il est conseillé au lecteur n'ayant pas ces connaissances de lire en premier l'annexe A.

Cette Recommandation est une extension du modèle de référence (Recommandation X.200) destinée à couvrir les aspects de sécurité qui sont des éléments généraux d'architecture des protocoles de communication, mais qui ne sont pas traités dans le modèle de référence.

1 Domaine d'application et objet

La présente Recommandation,

a) donne une description générale des services de sécurité et des mécanismes associés qui peuvent être fournis par le modèle de référence;

b) signale, dans le modèle de référence, les emplacements où les services et mécanismes peuvent être fournis.

La présente Recommandation élargit le champ d'application de la Recommandation X.200 afin de couvrir la sécurité des communications entre systèmes ouverts.

Des services et des mécanismes de sécurité de base ainsi que leur placement approprié ont été identifiés pour toutes les couches du modèle de référence. En outre, les relations architecturales entre les services et mécanismes de sécurité et le modèle de référence ont été identifiées. Des mesures supplémentaires de sécurité peuvent être nécessaires dans des systèmes d'extrémité, installations et organisations. Ces mesures s'appliquent dans différents contextes d'application. La définition des services de sécurité nécessaires à la prise en charge de ces mesures supplémentaires de sécurité ne relève pas du champ d'application de la présente Recommandation.

---

1) La Recommandation X.800 et la norme ISO 7498-2, Systèmes de traitement de l'information – Interconnexion des systèmes ouverts modèle de référence de base – Partie 2: Architecture de sécurité, sont alignées du point de vue technique.

Les fonctions de sécurité OSI ne concernent que les aspects visibles d'une voie de communication permettant aux systèmes d'extrémité de réaliser entre eux un transfert sûr d'informations. La sécurité OSI ne concerne pas des mesures de sécurité nécessaires dans les systèmes d'extrémité, installations et organisations, sauf lorsque ces mesures ont des effets sur le choix et le placement de services de sécurité visibles dans l'OSI. Ces derniers aspects de la sécurité peuvent être normalisés, mais pas le cadre des Recommandations relatives à l'OSI.

La présente Recommandation complète les concepts et principes définis dans la Recommandation X.200; elle ne les modifie pas. Elle ne constitue ni une spécification de réalisation de systèmes, ni une base d'évaluation de la conformité de réalisation de systèmes.

2 Références

Rec. X.200, Modèle de référence pour l'interconnexion des systèmes ouverts pour les applications du CCITT.

ISO 7498 – Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Modèle de référence de base

ISO 7498-4 – Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Modèle de référence de base – Partie 4: Cadre de gestion (1989).

ISO 7498/Add.1 – Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Modèle de référence de base – Addendum 1: Transmission en mode sans connexion (1987).

ISO 8648 – Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Organisation interne de la couche réseau (1988).

3 Définitions et abréviations

3.1 La présente Recommandation se fonde sur les concepts élaborés dans la Recommandation X.200 et utilise les termes suivants qui y sont définis:

a) connexion (N);

b) transmission de données (N);

c) entité (N);

d) facilité (N);

e) couche (N);

f) système ouvert;

g) entités homologues;

h) protocole (N);

j) unité de données de protocole (N);

k) relais (N);

l) routage;

m) maintien en séquence;

n) service (N);

p) unité de données de service (N);

q) données utilisateur (N);

r) sous-réseau;

s) ressource OSI;

t) syntaxe de transfert.

3.2 La présente Recommandation utilise les termes suivants, définis dans les Recommandations/normes internationales citées en référence.

Transmission en mode sans connexion (ISO 7498/Add.1)

Système d'extrémité (Rec. X.200 du CCITT/ISO 7498)

Fonction de relais et de routage (ISO 8648)

Base d'informations de gestion (MIB) (ISO 7498-4).

En outre, les abréviations suivantes sont utilisées:

OSI interconnexion de systèmes ouverts (Open Systems Interconnection)

SDU unité de données de service (Service Data Unit)

SMIB base d'informations de gestion de sécurité (Security Management Information Base)

MIB base d'informations de gestion (Management Information Base)

3.3 Pour les besoins de la présente Recommandation, les définitions suivantes s'appliquent:

3.3.1 **contrôle d'accès**

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.

3.3.2 **liste de contrôle d'accès**

Liste des entités qui sont autorisées à accéder à une ressource, avec leurs autorisations d'accès.

3.3.3 **imputabilité**

Propriété qui garantit que les actions d'une entité ne peuvent être imputées qu'à cette entité.

3.3.4 **menace active**

Menace de modification non autorisée et délibérée de l'état du système.

Remarque – La modification et la répétition de messages, l'insertion de faux messages, le déguisement d'une entité autorisée et le déni de service sont des exemples de menaces actives.

3.3.5 **audit**

Voir «audit de sécurité» (§ 3.3.47).

3.3.6 **enregistrement d'audit**

Voir «enregistrement d'audit de sécurité» (§ 3.3.48).

3.3.7 **authentification**

Voir «authentification de l'origine des données» et «authentification de l'entité homologue» (§ 3.3.22 et 3.3.40).

Remarque – Dans la présente Recommandation, le terme «authentification» n'est pas associé à l'intégrité des données; le terme «intégrité des données» est utilisé à la place.

3.3.8 **information d'authentification**

Information utilisée pour établir la validité d'une identité déclarée.

3.3.9 **échange d'authentification**

Mécanisme destiné à garantir l'identité d'une entité par échange d'informations.

3.3.10 **autorisation**

Attribution de droits, comprenant la permission d'accès sur la base de droits d'accès.

3.3.11 **disponibilité**

Propriété d'être accessible et utilisable sur demande par une entité autorisée.

3.3.12 **capacité**

Jeton utilisé comme identificateur d'une ressource de telle sorte que la possession du jeton confère des droits d'accès à cette ressource.

3.3.13 **voie**

Chemin de transfert de l'information.

3.3.14 **cryptogramme**

Données obtenues par l'utilisation du chiffrement. Le contenu sémantique des données résultantes n'est pas compréhensible.

Remarque – Le cryptogramme peut lui-même être réinjecté dans un nouveau chiffrement pour produire un cryptogramme surchiffré.

3.3.15 **texte en clair**

Données intelligibles dont la sémantique est compréhensible.

3.3.16 **confidentialité**

Propriété d'une information qui n'est ni disponible, ni divulguée aux personnes, entités ou processus non autorisés.

3.3.17 **justificatif d'identité**

Données transférées pour établir l'identité déclarée d'une entité.

3.3.18 **analyse cryptographique**

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).

3.3.19 **valeur de contrôle cryptographique**

Information obtenue en réalisant une transformation cryptographique sur une unité de données.

Remarque – La valeur de contrôle peut être obtenue en une ou plusieurs étapes et résulte d'une fonction mathématique utilisant la clé et une unité de données. Elle permet de vérifier l'intégrité d'une unité de données.

3.3.20 **cryptographie**

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.

Remarque – 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.

3.3.21 **intégrité des données**

Propriété assurant que des données n'ont pas été modifiées ou détruites de façon non autorisée.

3.3.22 **authentification de l'origine des données**

Confirmation que la source des données reçues est telle que déclarée.

3.3.23, 3.3.24 **déchiffrement**

Opération inverse d'un chiffrement réversible.

3.3.25 **déni de service**

Impossibilité d'accès à des ressources pour des utilisateurs autorisés ou introduction d'un retard pour le traitement d'opérations critiques.

3.3.26 **signature numérique**

Données ajoutées à une unité de données, ou transformation cryptographique d'une unité de données, permettant à un destinataire de prouver la source et l'intégrité de l'unité de données et protégeant contre la contrefaçon (par le destinataire, par exemple).

3.3.27, 3.3.28 **chiffrement**

Transformation cryptographique de données produisant un cryptogramme.

Remarque – Le chiffrement peut être irréversible. Dans ce cas, le déchiffrement correspondant ne peut pas être effectué.

3.3.29 **chiffrement de bout en bout**

Chiffrement de données à l'intérieur ou au niveau du système d'extrémité source, le déchiffrement correspondant ne se produisant qu'à l'intérieur, ou au niveau du système d'extrémité de destination (voir aussi le § 3.3.34).

3.3.30 **politique de sécurité fondée sur l'identité**

Politique de sécurité fondée sur les identités et/ou les attributs des utilisateurs, d'un groupe d'utilisateurs ou d'entités agissant au nom d'utilisateurs et sur les identités et/ou attributs des ressources/objets auxquels on doit accéder.

3.3.31 **intégrité**

Voir «intégrité des données» (§ 3.3.21).

3.3.32 **clé**

Série de symboles commandant les opérations de chiffrement et de déchiffrement.

3.3.33 **gestion de clés**

Production, stockage, distribution, suppression, archivage et application de clés conformément à la politique de sécurité.

3.3.34 **chiffrement de liaison (liaison par liaison)**

Application particulière du chiffrement à chaque liaison d'un système de communication (voir aussi «chiffrement de bout en bout», § 3.3.29).

Remarque – Le chiffrement liaison par liaison implique que les données soient du texte en clair dans les entités relais.

3.3.35 **détection de modification**

Mécanisme utilisé pour détecter les modifications, accidentelles ou intentionnelles, d'une unité de données.

3.3.36 **usurpation d'identité**

Prétention qu'a une entité d'en être une autre.

3.3.37 **notarisation**

Enregistrement de données chez un tiers de confiance permettant de s'assurer ultérieurement de leur exactitude (contenu, origine, date, remise).

3.3.38 **menace passive**

Menace d'une divulgation non autorisée des informations, sans que l'état du système ne soit modifié.

3.3.39 **mot de passe**

Information d'authentification confidentielle, habituellement composée d'une chaîne de caractères.

3.3.40 **authentification de l'entité homologue**

Confirmation qu'une entité homologue d'une association est bien l'entité déclarée.

3.3.41 **sécurité physique**

Mesures prises pour assurer la protection des ressources contre des menaces délibérées ou accidentelles.

3.3.42 **politique**

Voir «politique de sécurité» (§ 3.3.50).

3.3.43 **respect de la vie privée**

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.

Remarque – 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.

3.3.44 **répudiation**

Le fait, pour une des entités impliquées dans la communication, de nier avoir participé aux échanges, totalement ou en partie.

3.3.45 **contrôle de routage**

Application de règles, au cours du processus de routage, afin de choisir ou d'éviter, des réseaux, liaisons ou relais spécifiques.

3.3.46 **politique de sécurité fondée sur des règles**

Politique de sécurité fondée sur des règles globales imposées à tous les utilisateurs. Ces règles s'appuient généralement sur une comparaison de la sensibilité des ressources auxquelles on doit accéder avec les attributs correspondants d'utilisateurs, d'un groupe d'utilisateurs ou d'entités agissant au nom d'utilisateurs.

3.3.47 **audit de sécurité**

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.

3.3.48 **journal d'audit de sécurité**

Données collectées et pouvant éventuellement être utilisées pour permettre un audit de sécurité.

3.3.49 **étiquette de sécurité**

Marque liée à une ressource dénommant ou désignant les attributs de sécurité de cette ressource (cette ressource peut être une unité de données).

Remarque – La marque et/ou l'association de la marque à la ressource peuvent être implicites ou explicites.

3.3.50 **politique de sécurité**

Ensemble des critères permettant de fournir des services de sécurité [voir aussi «politique de sécurité fondée sur l'identité» (§ 3.3.30) et «politique de sécurité fondée sur des règles» (§ 3.3.46)].

Remarque – Une politique de sécurité complète traite nécessairement de sujets qui ne relèvent pas du champ d'application de l'OSI.

3.3.51 **service de sécurité**

Service, fourni par une couche de systèmes ouverts, garantissant une sécurité des systèmes et du transfert de données.

3.3.52 **protection sélective des champs**

Protection de certains champs spécifiques dans un message à transmettre.

3.3.53 **sensibilité**

Caractéristique d'une ressource relative à sa valeur ou à son importance et, éventuellement, à sa vulnérabilité.

3.3.54 **signature**

Voir «signature numérique» (§ 3.3.26).

3.3.55 **menace**

Violation potentielle de la sécurité.

3.3.56 **analyse du trafic**

Déduction d'informations à partir de l'observation des flux de données (présence, absence, quantité, direction, fréquence).

3.3.57 **confidentialité du flux de données**

Service de confidentialité fournissant une protection contre l'analyse du trafic.

3.3.58 **bourrage**

Production d'instances de communication parasites, d'unités de données parasites et/ou de données parasites dans des unités de données.

3.3.59 **Fonctionnalité de confiance**

Fonctionnalité perçue comme correcte en ce qui concerne certains critères, tels que ceux qui sont définis par une politique de sécurité, par exemple.

4 Notation

La notation utilisée pour désigner les couches est la même que celle qui est définie dans la Recommandation X.200 du CCITT.

Le terme «service» est utilisé pour se référer à un service de sécurité, sauf autre précision.

5 Description générale des services et des mécanismes de sécurité

5.1 *Aperçu général*

Les services de sécurité qui sont inclus dans l'architecture de sécurité OSI et les mécanismes mettant en oeuvre ces services sont présentés dans le présent paragraphe. Les services de sécurité décrits ci-dessous sont des services de sécurité de base. Dans la pratique, ils seront utilisés dans les couches appropriées et selon des combinaisons appropriées, généralement avec des services et des mécanismes non OSI, afin de satisfaire à la politique de sécurité et/ou aux exigences de l'utilisateur. On peut utiliser des mécanismes de sécurité particuliers pour mettre en œuvre des combinaisons de services de sécurité de base. Des réalisations pratiques de systèmes peuvent mettre en œuvre des combinaisons particulières de services de sécurité de base pouvant être appelés directement.

5.2 *Services de sécurité*

Les services suivants sont considérés comme étant des services de sécurité qui peuvent être fournis en option dans le cadre du modèle de référence OSI. Les services d'authentification nécessitent une information d'authentification comprenant des informations stockées localement et des données qui sont transférées (justificatif d'identité) pour faciliter l'authentification.

5.2.1 *Authentification*

Ces services assurent l'authentification d'une entité homologue communicante et l'authentification de la source des données, comme décrit ci-dessous.

5.2.1.1 *Authentification de l'entité homologue*

Lorsque ce service est fourni par la couche (N), il confirme à l'entité (N + 1) que l'entité homologue est bien l'entité (N + 1) déclarée.

Ce service est prévu pour être utilisé lors de l'établissement de la phase de transfert de données d'une connexion, ou parfois pendant cette phase, pour confirmer les identités d'une ou de plusieurs entités connectées à une ou plusieurs autres entités. Ce service garantit (uniquement lors de son utilisation) qu'une entité n'essaie pas d'usurper une identité ou de répéter une ancienne connexion de façon non autorisée. Des schémas d'authentification unilatérale ou mutuelle d'entité homologue, avec ou sans contrôle réitéré, sont possibles et peuvent donner divers degrés de protection.

5.2.1.2 *Authentification de l'origine des données*

Lorsque ce service est fourni par la couche (N), il confirme à une entité (N + 1) que la source des données est bien l'entité homologue (N + 1) déclarée.

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

5.2.2 *Contrôle d'accès*

Ce service assure une protection contre toute utilisation non autorisée des ressources accessibles via l'OSI. Celles-ci peuvent être des ressources OSI ou non OSI auxquelles on accède via des protocoles OSI. Ce service de protection peut être appliqué pour différents types d'accès à une ressource (par exemple, l'utilisation d'une ressource de communication; la lecture, l'écriture ou la suppression d'une ressource d'information; l'exécution d'une ressource de traitement) ou pour tous les accès à une ressource.

Le contrôle d'accès se fera conformément aux différentes politiques de sécurité (voir le § 6.2.1.1).

5.2.3 *Confidentialité des données*

Ces services assurent la protection des données contre toute divulgation non autorisée, comme décrit ci-dessous.

5.2.3.1 *Confidentialité des données en mode connexion*

Ce service assure la confidentialité de toutes les données utilisateur (N) au cours d'une connexion (N).

Remarque – Selon l'utilisation et la couche, il peut s'avérer approprié de protéger toutes les données, par exemple, les données exprès ou les données d'une demande de connexion.

5.2.3.2 *Confidentialité des données en mode sans connexion*

Ce service assure la confidentialité de toutes les données utilisateur (N) dans une unité de données de service (N) en mode sans connexion.

5.2.3.3 *Confidentialité sélective par champ*

Ce service assure la confidentialité de champs sélectionnés dans les données utilisateur (N) au cours d'une connexion (N) ou dans une unité de données de service (N) en mode sans connexion.

5.2.3.4 *Confidentialité du flux de données*

Ce service assure la protection des informations qui pourraient être dérivées de l'observation des flux de données.

5.2.4 *Intégrité des données*

Ces services contrecarrent les menaces actives et peuvent prendre l'une des formes décrites ci-dessous.

Remarque – L'utilisation du service d'authentification de l'entité homologue au début de la connexion et du service d'intégrité des données au cours de la connexion peuvent confirmer conjointement la source de toutes les unités de données transférées au cours de la connexion, l'intégrité de ces unités de données, et peuvent, en outre, assurer la détection de la duplication des unités de données, par l'utilisation de numéros de séquence, par exemple.

5.2.4.1 *Intégrité en mode connexion avec reprise*

Ce service assure l'intégrité de toutes les données utilisateur (N) au cours d'une connexion (N) et détecte toute donnée modifiée, insérée, supprimée ou répétée dans une séquence entière d'unité de données de service (avec tentative de reprise).

5.2.4.2 *Intégrité en mode connexion sans reprise*

Comme pour le § 5.2.4.1, mais sans tentative de reprise.

5.2.4.3 *Intégrité en mode connexion sélective par champ*

Ce service assure l'intégrité de champs sélectionnés dans les données utilisateur (N) d'une unité de données de service (N) au cours d'une connexion et prend la forme d'une indication permettant de savoir si les champs sélectionnés ont été modifiés, insérés, supprimés ou répétés.

5.2.4.4 *Intégrité en mode sans connexion*

Lorsque ce service est fourni par la couche (N), il donne l'assurance de l'intégrité à l'entité (N + 1) requérante.

Ce service assure l'intégrité d'une seule unité de données de service en mode sans connexion et peut prendre la forme d'une indication permettant de savoir si une unité de données de service reçue a été modifiée. En outre, une forme limitée de détection de donnée répétée peut être fournie.

5.2.4.5 *Intégrité en mode sans connexion sélective par champ*

Ce service assure l'intégrité de champs sélectionnés dans une unité de données de service en mode sans connexion et prend la forme d'une indication permettant de savoir si les champs sélectionnés ont été modifiés.

5.2.5 *Non-répudiation*

Ce service peut prendre l'une des deux formes suivantes ou les deux.

5.2.5.1 *Non-répudiation avec preuve de l'origine*

Le destinataire des données reçoit la preuve de l'origine des données. Cela le protégera de toute tentative de l'expéditeur de nier le fait qu'il a envoyé les données ou leur contenu.

5.2.5.2 *Non-répudiation avec preuve de la remise*

L'expéditeur des données reçoit la preuve de la remise des données. Cela le protégera contre toute tentative ultérieure du destinataire de nier le fait d'avoir reçu les données ou leur contenu.

5.3 *Mécanismes de sécurité spécifiques*

Les mécanismes suivants peuvent être incorporés dans la couche (N) appropriée pour fournir certains services décrits au § 5.2.

5.3.1 *Chiffrement*

5.3.1.1 Le chiffrement peut assurer la confidentialité soit des données, soit du flux de données et peut jouer un rôle dans un certain nombre d'autres mécanismes de sécurité ou les compléter comme le décrivent les paragraphes suivants.

5.3.1.2 Les algorithmes de chiffrement peuvent être réversibles ou irréversibles. Un algorithme de chiffrement réversible peut être de deux types:

a) chiffrement symétrique (c'est-à-dire à clé secrète), dans lequel la connaissance de la clé de chiffrement implique une connaissance de la clé de déchiffrement et vice versa;

b) chiffrement asymétrique (par exemple, à clé publique) dans lequel la connaissance de la clé de chiffrement n'implique pas la connaissance de la clé de déchiffrement, ou vice versa. Les deux clés de ce système sont parfois appelées «clé publique» et «clé privée».

Les algorithmes de chiffrement irréversibles peuvent ou non utiliser une clé. Lorsqu'ils utilisent une clé, celle-ci peut être publique ou secrète.

5.3.1.3 L'existence d'un mécanisme de chiffrement implique l'utilisation d'un mécanisme de gestion de clés, sauf dans le cas de certains algorithmes de chiffrement irréversibles. Le § 8.4 donne certains principes directeurs sur la méthodologie de gestion de clés.

5.3.2 *Mécanismes de signature numérique*

Ces mécanismes définissent deux procédures:

a) signature d'une unité de données;

b) vérification d'une unité de données signée.

Le premier processus utilise une information qui est privée (c'est-à-dire unique et confidentielle) pour le signataire. Le second processus utilise des procédures et une information qui sont disponibles dans le public, mais desquelles on ne peut pas déduire l'information privée du signataire.

5.3.2.1 Le processus de signature implique soit un chiffrement de l'unité de données, soit la production d'une valeur de contrôle cryptographique de l'unité de données, en utilisant l'information privée du signataire comme une clé privée.

5.3.2.2 Le processus de vérification implique l'utilisation de procédures et d'informations publiques pour déterminer si la signature a été produite avec l'information privée du signataire.

5.3.2.3 La caractéristique essentielle du mécanisme de signature est que la signature ne peut être produite qu'en utilisant l'information privée du signataire. Par conséquent, lorsqu'on vérifie la signature, on peut prouver, par la suite, à une tierce partie (par exemple, un juge ou un arbitre), à tout moment, que seul le détenteur unique de l'information privée peut avoir produit la signature.

5.3.3 *Mécanismes de contrôle d'accès*

5.3.3.1 Ces mécanismes peuvent utiliser l'identité authentifiée d'une entité ou des informations relatives à l'entité (telle que l'appartenance à un ensemble connu d'entités) ou des capacités de l'entité pour déterminer et appliquer les droits d'accès de l'entité. Si l'entité essaie d'utiliser une ressource non autorisée, ou une ressource utilisée avec un type d'accès incorrect, la fonction de contrôle d'accès rejettera cette tentative et pourra en outre consigner l'incident afin de générer une alarme et/ou de l'enregistrer dans le journal d'audit de sécurité. Toute notification à l'expéditeur d'un refus d'accès pour une transmission de données en mode sans connexion ne peut être fournie qu'à la suite de contrôles d'accès imposés à l'origine.

5.3.3.2 Les mécanismes de contrôle d'accès peuvent, par exemple, être basés sur l'utilisation d'un ou de plusieurs des éléments suivants:

a) bases d'informations de contrôle d'accès où sont gardés les droits d'accès des entités homologues. Ces informations peuvent être conservées par des centres d'autorisation ou par l'entité à laquelle on a accès et peuvent avoir la forme d'une liste de contrôle d'accès ou d'une matrice de structure hiérarchique ou répartie. Cela présuppose que l'authentification de l'entité homologue ait été assurée;

b) informations d'authentification telles que mots de passe, dont la possession et la présentation ultérieure sont la preuve que l'entité qui effectue l'accès y est autorisée;

c) capacités, dont la possession et la présentation ultérieure sont la preuve du droit à l'accès à l'entité ou à la ressource définie par la capacité;

Remarque – Une capacité devrait être infalsifiable et devrait être acheminée d'une manière sûre.

d) étiquettes de sécurité qui, lorsqu'elles sont associées à une entité, peuvent être utilisées pour accorder ou refuser l'accès, en général conformément à une politique de sécurité;

e) heure de la tentative d'accès;

f) route de la tentative d'accès;

g) durée de l'accès.

5.3.3.3 Des mécanismes de contrôle d'accès peuvent être appliqués à l'une ou l'autre extrémité d'une association de communication et/ou en tout point intermédiaire.

Les contrôles d'accès effectués à l'origine ou en tout point intermédiaire sont utilisés pour déterminer si l'expéditeur est autorisé à communiquer avec le destinataire et/ou à utiliser les ressources de communications requises.

Pour une transmission de données en mode sans connexion, les besoins en mécanismes de contrôle d'accès de l'entité destinataire doivent être connus a priori du côté de l'entité source. Ces besoins doivent être enregistrés dans la base d'informations de gestion de sécurité (voir les § 6.2 et 8.1).

5.3.4 *Mécanismes d'intégrité des données*

5.3.4.1 Il y a deux aspects de l'intégrité des données: l'intégrité d'une seule unité de données ou d'un seul champ d'unité de données et l'intégrité d'un train d'unités de données ou d'un train de champ d'unités de données. En général, différents mécanismes sont utilisés pour fournir ces deux types de service d'intégrité, bien que la fourniture du second sans le premier ne soit pas possible.

5.3.4.2 La détermination de l'intégrité d'une unité de données unique implique deux processus, l'un au niveau de l'entité émettrice et l'autre au niveau de l'entité réceptrice. L'entité émettrice ajoute à une unité de données une grandeur qui est une fonction de la donnée. Cette grandeur peut être une information supplémentaire, tel qu'un code de contrôle par bloc ou une valeur de contrôle cryptographique, et peut elle-même être chiffrée. L'entité réceptrice génère une quantité correspondante et la compare à la grandeur reçue pour déterminer si les données ont été modifiées pendant le transit. Ce mécanisme seul ne protégera par contre pas, contre la répétition d'une seule unité de données. Dans les couches appropriées de l'architecture, la détection d'une manipulation peut conduire à une action de reprise (par exemple, via une retransmission ou une correction d'erreur) au niveau de cette couche ou au niveau d'une couche supérieure.

5.3.4.3 Pour le transfert de données en mode connexion, la protection de l'intégrité d'une séquence d'unités de données (c'est-à-dire, la protection contre les erreurs de séquencement, la perte, la répétition, l'insertion ou la modification de données) nécessite en outre une certaine forme de séquencement explicite telle que la numérotation de séquence, l'horodatage ou le chaînage cryptographique.

5.3.4.4 Pour la transmission de données en mode sans connexion, l'horodatage peut être utilisé pour assurer une forme de protection limitée contre le fait de répéter des unités de données individuelles.

5.3.5 *Mécanisme d'échange d'authentification*

5.3.5.1 Certaines des techniques qui peuvent être appliquées aux échanges d'authentification sont les suivantes:

a) utilisation d'information d'authentification, telle que mots de passe – fournis par une entité émettrice et contrôlés par l'entité réceptrice;

b) techniques cryptographiques;

c) utilisation de caractéristiques et/ou de ce qui est propre à l'entité.

5.3.5.2 Les mécanismes peuvent être incorporés dans la couche (N) afin d'assurer l'authentification de l'entité homologue. Si le mécanisme ne réussit pas à authentifier l'entité, cela provoquera le rejet ou la terminaison de la connexion et cela peut également provoquer une entrée dans le journal d'audit de sécurité et/ou un rapport au centre de gestion de la sécurité.

5.3.5.3 Lorsque des techniques cryptographiques sont utilisées, elles peuvent être combinées à des protocoles «d'échanges interactifs» pour se protéger contre le fait de répéter (c'est-à-dire, pour s'assurer d'une présence effective).

5.3.5.4 Le choix des techniques d'échange d'authentification dépendra des circonstances dans lesquelles elles seront utilisées. Très souvent, il sera nécessaire de les utiliser avec:

a) horodatage et horloges synchronisées;

b) deux et trois échanges (respectivement pour l'authentification unilatérale et mutuelle);

c) des services de non-répudiation réalisés par signature numérique et/ou mécanismes de notarisation.

5.3.6 *Mécanisme de bourrage*

Les mécanismes de bourrage peuvent être utilisés pour assurer différents niveaux de protection contre l'analyse du trafic. Ce mécanisme ne peut être efficace que si le bourrage est protégé par un service de confidentialité.

5.3.7 *Mécanisme de contrôle de routage*

5.3.7.1 Les routes peuvent être choisies soit de façon dynamique, soit par arrangement préalable de façon à n'utiliser que des sous-réseaux, relais ou liaisons physiquement sûrs.

5.3.7.2 Les systèmes d'extrémité peuvent, lors de la détection d'attaques persistantes par manipulation, souhaiter demander au fournisseur du service de réseau d'établir une connexion via une route différente.

5.3.7.3 La politique de sécurité peut interdire le passage de données portant certaines étiquettes de sécurité à travers certains sous-réseaux, relais ou liaisons. L'initiateur d'une connexion (ou l'expéditeur d'une unité de données en mode sans connexion) peut aussi spécifier des interdictions de routage prescrivant d'éviter des sous-réseaux, liaisons ou relais spécifiques.

5.3.8 *Mécanismes de notarisation*

5.3.8.1 Des propriétés relatives à des données communiquées entre deux entités ou plus, telles que leur intégrité, leur origine, leur date et leur destination, peuvent être garanties par la fourniture d'un mécanisme de notarisation. La garantie est fournie par un notaire (tierce partie) en qui les entités communicantes ont confiance et qui détient les informations nécessaires pour fournir la garantie requise de manière vérifiable. Chaque instance de communication peut utiliser la signature numérique, le chiffrement et les mécanismes d'intégrité, de façon appropriée, pour le service que doit fournir le notaire. Lorsqu'on fait appel à ce mécanisme de notarisation, les données sont communiquées entre les entités communicantes via les instances de communication protégées et le notaire.

5.4 *Mécanismes de sécurité communs*

Le présent paragraphe décrit un certain nombre de mécanismes qui ne sont pas spécifiques à un service particulier. Ainsi, au § 7, ils ne sont pas décrits explicitement comme faisant partie d'une couche particulière. Certains de ces mécanismes de sécurité communs peuvent être considérés comme des aspects de gestion de sécurité (voir également le § 8). L'importance de ces mécanismes est, en général, directement liée au niveau de sécurité requis.

5.4.1 *Fonctionnalités de confiance*

5.4.1.1 Des fonctionnalités de confiance doivent être utilisées pour étendre le domaine d'application ou pour établir l'efficacité d'autres mécanismes de sécurité. Toute fonctionnalité qui fournit directement des mécanismes de sécurité, ou qui permet l'accès à ces mécanismes, devrait être digne de confiance.

5.4.1.2 Les procédures utilisées pour assurer que l'on peut faire confiance à un matériel et un logiciel n'entrent pas dans le cadre de la présente Recommandation et, en tout cas, varient selon le niveau de menace perçu et la valeur des informations à protéger.

5.4.1.3 Ces procédures sont en général coûteuses et difficiles à mettre en œuvre. On peut réduire au minimum les problèmes en choisissant une architecture qui permette la mise en œuvre de fonctions de sécurité en modules qui peuvent être séparés des fonctions non liées à la sécurité ou fournis par elles.

5.4.1.4 Toute protection d'associations au-dessus de la couche sur laquelle porte la protection doit être fournie par d'autres moyens, par exemple, par une fonctionnalité de confiance appropriée.

5.4.2 *Etiquettes de sécurité*

5.4.2.1 Les ressources comprenant des éléments de données peuvent avoir des étiquettes de sécurité qui leur sont associées, par exemple, pour indiquer un niveau de sensibilité. Il est souvent nécessaire d'acheminer l'étiquette de sécurité appropriée avec des données en transit. Une étiquette de sécurité peut être une donnée supplémentaire associée aux données transférées ou peut être implicite; elle peut, par exemple, être la conséquence de l'utilisation d'une clé spécifique pour chiffrer les données ou résulter du contexte des données tel que la source ou la route. Les étiquettes de sécurité explicites doivent être clairement identifiables afin de pouvoir être vérifiées de façon appropriée. En outre, elles doivent être liées d'une manière sûre aux données auxquelles elles sont associées.

5.4.3 *Détection d'événements*

5.4.3.1 La détection d'événements liés à la sécurité comprend la détection de violations apparentes de la sécurité et peut également inclure la détection d'événements «normaux», tels que l'accès réussi (ou demande de connexion). Dans l'OSI, les événements liés à la sécurité peuvent être détectés par des entités comprenant des mécanismes de sécurité. La spécification de ce qui constitue un événement est mise à jour par la gestion du traitement d'événements (voir le § 8.3.1). La détection des divers événements liés à la sécurité peut, par exemple, provoquer une ou plusieurs des actions suivantes:

a) notification locale de l'événement;

b) notification à distance de l'événement;

c) enregistrement de l'événement (voir le § 5.4.3);

d) action de reprise (voir le § 5.4.4).

Les exemples d'événements liés à la sécurité sont les suivants:

a) une violation spécifique de la sécurité;

b) un événement spécifique choisi;

c) un dépassement du comptage d'un certain nombre d'occurrences.

5.4.3.2 La normalisation dans ce domaine tiendra compte de la transmission des informations pertinentes pour la notification et l'enregistrement d'événements, et de la définition syntaxique et sémantique à utiliser pour la transmission de notifications et d'enregistrements d'événements.

5.4.4 *Journal d'audit de sécurité*

5.4.4.1 Les journaux d'audit de sécurité fournissent un mécanisme de sécurité appréciable étant donné qu'ils permettent potentiellement de détecter et d'enquêter sur les violations de sécurité en permettant un audit de sécurité ultérieur. Un audit de sécurité est une étude indépendante et un examen des enregistrements et des activités de système permettant de tester l'adéquation des contrôles, de s'assurer de la cohérence avec la politique établie et avec les procédures opérationnelles, d'aider à évaluer les dommages et de recommander des modifications dans les contrôles de la politique et les procédures. Un audit de sécurité nécessite l'enregistrement des informations relatives à la sécurité dans un journal d'audit de sécurité, ainsi que l'analyse et la production de rapports à partir des informations provenant d'un journal d'audit de sécurité. L'enregistrement est considéré comme un mécanisme de sécurité; il est donc décrit dans ce paragraphe. L'analyse et la production de rapports sont considérées comme une fonction de gestion de sécurité (voir le § 8.3.2).

5.4.4.2 La collecte d'informations pour le journal d'audit de sécurité peut être adaptée à divers besoins en spécifiant le(s) type(s) d'événements relatifs à la sécurité à enregistrer (par exemple, violations apparentes de la sécurité ou exécution d'opérations réussies).

L'existence connue d'un journal d'audit de sécurité peut servir d'élément dissuasif pour certaines sources potentielles d'attaques de sécurité.

5.4.4.3 Les considérations liées à un journal d'audit de sécurité OSI tiendront compte du type d'information qui pourra, en option, être enregistrée, des conditions sous lesquelles cette information devra être enregistrée et de la définition syntaxique et sémantique à utiliser pour échanger des informations de journal d'audit de sécurité.

5.4.5 *Reprise de sécurité*

5.4.5.1 La reprise de sécurité traite des demandes provenant de mécanismes tels que les fonctions de traitement et de gestion des événements et entreprend des actions de reprise comme résultat de l'application d'un ensemble de règles. Ces actions de reprise peuvent être de trois types:

a) immédiates;

b) temporaires;

c) à long terme.

Par exemple:

des actions immédiates peuvent créer une coupure immédiate des opérations, comme une déconnexion;

des actions temporaires peuvent produire l'invalidation temporaire d'une entité;

des actions à long terme peuvent être l'introduction d'une entité sur une «liste noire» ou le changement d'une clé.

5.4.5.2 Les sujets qui se prêtent à la normalisation comprennent des protocoles pour les actions de reprise et pour la gestion de reprise de sécurité (voir le § 8.3.3).

5.5 *Illustration de la relation entre services et mécanismes de sécurité*

Le tableau 1/X.800 montre les mécanismes qui, seuls ou combinés à d'autres, sont considérés comme étant parfois indiqués pour la fourniture de chaque service. Ce tableau présente un aperçu de ces relations et n'est pas définitif. Les services et mécanismes dont il est question dans ce tableau sont décrits aux § 5.2 et 5.3. Les relations sont décrites plus complètement au § 6.

TABLEAU 1/X.800

Illustration de la relation entre services de sécurité et mécanismes de sécurité

Mécanisme / Service	Chiffrement	Signature numérique	Contrôle d'accès	Intégrité des données	Echange d'authen-tification	Bourrage	Contrôle de routage	Notari-sation
Authentification de l'entité homologue	O	O	ù	ù	O	ù	ù	ù
Authentification de l'origine des données	O	O	ù	ù	ù	ù	ù	ù
Service de contrôle d'accès	ù	ù	O	ù	ù	ù	ù	ú
Confidentialité en mode connexion	O	ù	ù	ù	ù	ù	O	ù
Confidentialité en mode sans connexion	O	ù	ù	ù	ù	ù	O	ù
Confidentialité sélective par champ	O	ù	ù	ù	ù	ù	ù	ù
Confidentialité du flux de données	O	ù	ù	ù	ù	O	O	ù
Intégrité en mode connexion avec reprise	O	ù	ù	O	ù	ù	ù	ù
Intégrité en mode connexion sans reprise	O	ù	ù	O	ù	ù	ù	ù
Intégrité en mode connexion sélective par champ	O	ù	ù	O	ù	ù	ù	ù
Intégrité en mode sans connexion	O	O	ù	O	ù	ù	ù	ù
Intégrité en mode sans connexion sélective par champ	O	O	ù	O	ù	ù	ù	ù
Non-répudiation origine	ù	O	ù	O	ù	ù	ù	O
Non-répudiation remise	ù	O	ù	O	ù	ù	ù	O

ù Le mécanisme est considéré comme inapproprié.

O Oui. Le mécanisme est approprié, soit individuellement, soit combiné à d'autres mécanismes.

Remarque – Dans certains cas, le mécanisme prévoit bien plus de fonctions que celles qui sont nécessaires pour tel ou tel service, mais ne peut cependant pas être utilisé.

6 Relation entre services, mécanismes et couches

6.1 *Principes de la répartition des services et mécanismes de sécurité dans les couches*

6.1.1 Les principes suivants ont été utilisés en vue de déterminer l'affectation des services de sécurité aux couches et le placement des mécanismes de sécurité dans les couches:

a) réduire au minimum le nombre de possibilités différentes pour réaliser un service;

b) construire des systèmes sûrs en fournissant des services de sécurité dans plus d'une couche;

c) éviter que les fonctionnalités supplémentaires nécessaires pour la sécurité ne dupliquent sans raison les fonctions OSI existantes;

d) éviter toute violation de l'indépendance des couches;

e) réduire au minimum la quantité de fonctionnalités de confiance;

f) chaque fois qu'une entité dépend d'un mécanisme de sécurité fourni par une entité dans une couche inférieure, construire toute couche intermédiaire de façon que toute violation de la sécurité soit impossible;

g) chaque fois que cela est possible, définir les fonctions supplémentaires de sécurité d'une couche de façon à ne pas empêcher la mise en œuvre sous forme d'un (de) module(s) autonome(s);

h) pouvoir appliquer la présente Recommandation aux systèmes ouverts constitués de systèmes d'extrémité contenant les sept couches et aux systèmes relais.

6.1.2 Les demandes de services de sécurité peuvent rendre nécessaire une modification des définitions de service au niveau de chaque couche, que les services de sécurité demandés soient fournis au niveau de cette couche ou au-dessous.

6.2 *Modèle d'appel, de gestion et d'utilisation des services (N) protégés*

Il convient de lire le présent paragraphe en relation avec le § 8 qui contient une présentation d'ordre général sur les problèmes de gestion de sécurité. Il est prévu que les services et mécanismes de sécurité puissent être activés par l'entité de gestion via l'interface de gestion et/ou par l'appel du service.

6.2.1 *Détermination des caractéristiques de protection pour une instance de communication*

6.2.1.1 *Considérations générales*

Le présent paragraphe décrit l'appel de la protection des instances de communication en mode connexion et mode sans connexion. Dans le cas d'une communication en mode connexion, les services de protection sont généralement demandés/accordés au moment de l'établissement de la connexion. Dans le cas d'un appel de service en mode sans connexion, la protection est demandée/accordée pour chaque cas de demande de service sans connexion.

Pour simplifier la description suivante, le terme «demande de service» sera utilisé dans le sens de l'établissement d'une connexion, ou d'une demande de service sans connexion. L'appel de protection des données choisies peut être réalisé en demandant une protection sélective par champ. Par exemple, cela peut être réalisé moyennant l'établissement de plusieurs connexions, chacune ayant un type ou un niveau de protection différent.

Cette architecture de sécurité admet toute une gamme de politiques de sécurité, y compris celles qui se fondent sur des règles, celles qui se fondent sur des identités et celles qui sont une combinaison des deux. L'architecture de sécurité admet aussi des protections qui sont imposées administrativement, celles qui sont choisies dynamiquement et une combinaison des deux.

6.2.1.2 *Demandes de service*

Pour chaque demande de service (N), l'entité (N + 1) peut demander la protection de sécurité cible désirée. La demande de service (N) spécifiera les services de sécurité ainsi que les paramètres et toute information pertinente supplémentaire (telle que des informations sur la sensibilité et/ou les étiquettes de sécurité) pour réaliser la protection de sécurité cible.

Avant chaque instance de communication, la couche (N) doit avoir accès à la base d'informations de gestion de sécurité (SMIB) (voir le § 8.1). La SMIB contient des informations sur les demandes de protection imposées administrativement qui sont associées à l'entité (N + 1). Des fonctionnalités de confiance sont requises pour mettre en vigueur ces demandes de sécurité imposées administrativement.

La fourniture des caractéristiques de sécurité au cours d'une instance de communication en mode connexion peut nécessiter la négociation des services de sécurité qui sont requis. Les procédures requises pour négocier les mécanismes et les paramètres peuvent être exécutées soit séparément, soit comme faisant partie intégrante de la procédure normale d'établissement de la connexion.

Lorsque la négociation est exécutée séparément, les résultats de l'accord (portant sur le type de mécanisme de sécurité et les paramètres de sécurité nécessaires pour fournir ces services de sécurité) sont entrés dans la base d'informations de gestion de sécurité (voir le § 8.1).

Lorsque la négociation est effectuée comme faisant partie intégrante de la procédure normale d'établissement de la connexion, les résultats de la négociation entre les entités (N) seront provisoirement stockés dans la SMIB. Avant la négociation, chaque entité (N) aura accès à la SMIB pour obtenir toute information nécessaire à la négociation.

La couche (N) rejettera la demande de service si elle viole les demandes imposées administrativement qui sont enregistrées dans la SMIB pour l'entité (N + 1).

La couche (N) ajoutera également aux services de protection demandés tout service de sécurité défini dans la SMIB comme étant obligatoire pour obtenir la protection de sécurité cible.

Si l'entité (N + 1) ne spécifie pas de protection de sécurité cible, la couche (N) suivra une politique de sécurité conformément aux informations de la SMIB. Cette politique pourrait consister à poursuivre une communication en utilisant une protection par défaut conforme avec ce qui est défini pour l'entité (N + 1) dans la SMIB.

6.2.2 *Fourniture des services de protection*

Après avoir déterminé la combinaison des demandes de sécurité imposées administrativement et celles qui sont choisies dynamiquement, comme le décrit le § 6.2.1, la couche (N) essaiera de réaliser au moins la protection cible. Cela se fera par l'une des deux méthodes suivantes ou par les deux:

a) appel de mécanismes de sécurité directement dans la couche (N); et/ou

b) demande de services de protection à la couche (N – 1). Dans ce cas, le domaine de protection doit être étendu au service (N) par une combinaison de fonctionnalités de confiance et/ou de mécanismes de sécurité spécifiques de la couche (N).

Remarque – Ceci n'implique pas nécessairement que toutes les fonctionnalités de la couche (N) doivent être de confiance.

Ainsi, la couche (N) détermine si elle est capable de réaliser la protection cible requise. Si elle n'en n'est pas capable, aucune instance de communication ne se réalise.

6.2.2.1 *Etablissement d'une connexion (N) protégée*

La fourniture de services au sein de la couche (N) (au lieu de compter sur des services (N – 1)) est expliquée ci-après.

Dans certains protocoles, pour réaliser une protection cible satisfaisante, l'enchaînement des opérations est crucial.

a) *Contrôle d'accès sortant*

   La couche (N) peut imposer des contrôles d'accès sortant; c'est-à-dire: elle peut déterminer localement (à partir d'informations de la SMIB) si l'établissement de la connexion (N) protégée peut être tenté ou bien si cela est interdit.

b) *Authentification de l'entité homologue*

   Si la protection cible comprend une authentification de l'entité homologue, ou si l'on sait (par la SMIB) que l'entité (N) destinataire nécessitera une authentification de l'entité homologue, un échange d'authentification doit alors avoir lieu. Celui-ci peut utiliser deux ou trois échanges pour assurer une authentification unilatérale ou mutuelle, selon les besoins.

   Parfois, l'échange d'authentification peut être intégré dans les procédures habituelles d'établissement de la connexion (N). Dans d'autres circonstances, l'échange d'authentification peut être séparé de l'établissement de la connexion (N).

c) *Service de contrôle d'accès*

L'entité destinataire (N) ou les entités intermédiaires peuvent imposer des restrictions de contrôle d'accès. Si des informations spécifiques sont requises par un mécanisme de contrôle d'accès à distance, l'entité (N) initiatrice fournit ces informations dans le protocole de la couche (N) ou via la gestion de couche.

d) *Confidentialité*

Si un service de confidentialité totale ou sélective a été choisi, une connexion (N) protégée doit être établie. Ceci doit comprendre l'établissement de la (des) clé(s) de travail appropriée(s) et la négociation des paramètres cryptographiques pour la connexion. Ceci peut avoir été réalisé par arrangement préalable, dans l'échange d'authentification, ou par un protocole séparé.

e) *Intégrité des données*

Si l'intégrité de toutes les données utilisateur (N) avec ou sans reprise, ou l'intégrité sélective par champs a été choisie, une connexion protégée (N) doit être établie. Il peut s'agir de la même connexion que celle qui est établie pour fournir le service de confidentialité et cela peut permettre l'authentification. Les considérations concernant une connexion protégée applicables au service de confidentialité s'appliquent aussi au service d'intégrité des données.

f) *Services de non-répudiation*

Si la non-répudiation avec preuve de l'origine a été choisie, les paramètres cryptographiques appropriés ou une connexion protégée avec une entité de notarisation, doivent être établis.

Si la non-répudiation avec preuve de la remise a été choisie, les paramètres appropriés (qui sont différents de ceux requis pour la non-répudiation avec preuve de l'origine) ou une connexion protégée avec une entité de notarisation, doivent être établis.

Remarque – L'établissement de la connexion (N) protégée peut échouer par manque d'accord sur les paramètres cryptographiques (y compris éventuellement la nonpossession des clés appropriées) ou à cause du rejet par un mécanisme de contrôle d'accès.

6.2.3 *Fonctionnement d'une connexion (N) protégée*

6.2.3.1 Pendant la phase de transfert des données d'une connexion (N) protégée, les services de protection négociés doivent être fournis.

Les éléments suivants seront visibles à la frontière du service (N):

a) authentification de l'entité homologue (à intervalles réguliers);

b) protection sélective par champ;

c) notification d'attaque active (par exemple, lorsqu'une manipulation des données s'est produite et que le service fourni est «intégrité de la connexion sans reprise» – voir le § 5.2.4.2).

En outre, les éléments suivants peuvent être nécessaires:

a) enregistrement dans le journal d'audit de sécurité;

b) détection et traitement d'événements.

6.2.3.2 *Les services qui relèvent de l'application sélective sont:*

a) la confidentialité;

b) l'intégrité des données (éventuellement avec authentification);

c) la non-répudiation (par le destinataire ou par l'expéditeur).

Remarque 1 – Deux techniques sont suggérées pour marquer les éléments de données choisis pour l'application d'un service: la première implique l'utilisation de types spécifiques. On suppose que la couche présentation reconnaîtra certains types comme étant ceux qui nécessitent l'application de certains services de protection. La seconde comporte une certaine forme de signalisation des éléments de données individuels auxquels des services de protection spécifiques doivent être appliqués.

Remarque 2 – On suppose que l'une des raisons qui justifient l'application sélective de services de non-répudiation peut provenir du scénario suivant: une forme de dialogue de négociation apparaît par le biais d'une association avant que les deux entités (N) n'acceptent qu'une version finale d'un élément de données soit mutuellement acceptable. A ce moment-là, le destinataire prévu peut demander à l'expéditeur d'appliquer des services de non-répudiation (avec preuve de l'origine et de la remise) à la version finale acceptée de l'élément de données. L'expéditeur demande et obtient ces services et transmet l'élément de données; il est ensuite averti que l'élément de données a été reçu par le destinataire qui en a accusé réception. Les services de non-répudiation assurent à la fois l'expéditeur et le destinataire de l'élément de données que celui-ci a été transmis avec succès.

Remarque 3 – Les deux services de non-répudiation (c'est-à-dire avec preuve de l'origine et de la remise) sont appelés par l'expéditeur.

6.2.4 *Fourniture de la transmission protégée de données en mode sans connexion*

Les services de sécurité disponibles dans les protocoles en mode connexion ne sont pas tous disponibles dans les protocoles en mode sans connexion. Plus spécifiquement, une protection contre la suppression, l'insertion et la répétition si nécessaire, doit être fournie au niveau des couches supérieures qui sont, elles, en mode connexion. Une protection limitée contre la répétition, peut être fournie par un mécanisme d'horodatage. En outre, un certain nombre d'autres services de sécurité ne peuvent pas assurer le même degré de sécurité que celui qui est obtenu par des protocoles en mode connexion.

Les services de protection appropriés à la transmission de données en mode sans connexion sont les suivants:

a) authentification de l'entité homologue (voir le § 5.2.1.1);

b) authentification de l'origine des données (voir le § 5.2.1.2);

c) service de contrôle d'accès (voir le § 5.2.2);

d) confidentialité en mode sans connexion (voir le § 5.2.3.2);

e) confidentialité sélective par champ (voir le § 5.2.3.3);

f) intégrité en mode sans connexion (voir le § 5.2.4.4);

g) intégrité en mode sans connexion sélective par champ (voir le § 5.2.4.5);

h) non-répudiation, origine (voir le § 5.2.5.1).

Les services sont fournis par le chiffrement, des mécanismes de signature, des mécanismes de contrôle d'accès, des mécanismes de routage, des mécanismes d'intégrité des données et/ou des mécanismes de notarisation (voir le § 5.3).

L'initiateur d'une transmission de données en mode sans connexion devra s'assurer que son unité de données de service contient toutes les informations requises pour la rendre acceptable par le destinataire.

7 Placement des services et mécanismes de sécurité

Le présent paragraphe définit les services de sécurité à fournir dans le cadre du modèle de référence de base OSI et souligne la façon dont ils doivent être réalisés. La fourniture de tout service de sécurité est facultative, selon les besoins.

Lorsqu'un service de sécurité spécifique est identifié dans le présent paragraphe comme étant fourni en option par une couche particulière, le service de sécurité est fourni par des mécanismes de sécurité fonctionnant dans cette couche, sauf spécification contraire. Comme le décrit le § 6, plusieurs couches offriront de fournir des services de sécurité particuliers. Il se peut que ces couches ne fournissent pas toujours les services de sécurité par elles-mêmes, mais elles peuvent utiliser les services de sécurité appropriés qui sont fournis dans les couches inférieures. Même lorsque aucun service de sécurité n'est fourni dans une couche, la définition du service de cette couche peut devoir être modifiée pour permettre que des demandes de services de sécurité soient adressées à la couche inférieure.

Remarque 1 – Les mécanismes de sécurité communs (voir le § 5.4) ne sont pas traités dans le présent paragraphe.

Remarque 2 – Le choix du placement des mécanismes de chiffrement pour les applications est traité dans l'annexe C.

7.1 *Couche physique*

7.1.1 *Services*

Les seuls services de sécurité fournis au niveau de la couche physique, que ce soit individuellement ou combinés, sont les suivants:

a) confidentialité en mode connexion;

b) confidentialité de flux de données.

Le service de confidentialité du flux de données prend deux formes:

1) confidentialité totale du flux de données, laquelle ne peut être fournie que dans certaines circonstances, par exemple transmission bidirectionnelle simultanée, synchrone, point à point;

2) confidentialité limitée du flux de données, laquelle peut être fournie pour d'autres types de transmission, par exemple transmission asynchrone.

Ces services de sécurité sont limités aux menaces passives et peuvent être appliqués aux communications point à point ou multipoint.

7.1.2 *Mécanismes*

Le chiffrement total du flux de données est le principal mécanisme de sécurité au niveau de la couche physique.

L'une des formes de chiffrement, applicable uniquement au niveau de la couche physique, est la sécurité de transmission (c'est-à-dire, une sécurité à spectre étalé).

La protection de la couche physique est fournie par un dispositif de chiffrement qui fonctionne de façon transparente. L'objectif de la protection de la couche physique est de protéger tout le train binaire de données du service physique et de fournir la confidentialité du flux de données.

7.2 *Couche liaison de données*

7.2.1 *Services*

Les seuls services de sécurité fournis au niveau de la couche liaison de données sont:

a) la confidentialité en mode connexion;

b) la confidentialité en mode sans connexion.

7.2.2 *Mécanismes*

Le mécanisme de chiffrement est utilisé pour fournir les services de sécurité dans la couche liaison de données (voir l'annexe C).

La fonctionnalité de protection de sécurité de la couche de liaison est réalisée avant les fonctions normales de couche pour la transmission et après ces fonctions pour la réception, c'est-à-dire que les mécanismes de sécurité sont construits à partir de toutes les fonctions normales de la couche et utilisent ces fonctions.

Les mécanismes de chiffrement au niveau de la couche liaison de données sont sensibles au protocole de la couche liaison de données.

7.3 *Couche réseau*

L'organisation interne de la couche réseau permet qu'un ou plusieurs protocole(s) exécute(nt) différents rôles ou fonctions:

a) accès au sous-réseau;

b) convergence dépendant du sous-réseau;

c) convergence ne dépendant pas du sous-réseau;

d) relais et routage.

7.3.1 *Services*

Les services de sécurité qui peuvent être fournis, associés à la fourniture du service de réseau OSI, par le protocole d'accès au sous-réseau, sont les suivants:

a) authentification de l'entité homologue;

b) authentification de l'origine des données;

c) service de contrôle d'accès;

d) confidentialité en mode connexion;

e) confidentialité en mode sans connexion;

f) confidentialité du flux de données;

g) intégrité en mode connexion sans reprise;

h) intégrité en mode sans connexion.

Ces services de sécurité peuvent être fournis individuellement ou combinés. Les services de sécurité qui peuvent être fournis par le protocole responsable des opérations de relais de routage associées à la fourniture du service de réseau OSI, entre systèmes d'extrémité sont les mêmes que ceux qui sont assurés par le protocole responsable de l'accès au sous-réseau.

7.3.2 *Mécanismes*

7.3.2.1 Des mécanismes de sécurité identiques sont utilisés par le(s) protocole(s) qui effectue(nt) les opérations d'accès au sous-réseau, de relais et de routage associées à la fourniture du service de réseau OSI entre systèmes d'extrémité. Le routage est effectué dans cette couche, et le contrôle de routage est donc situé dans cette couche. Les services de sécurité identifiés sont fournis comme suit:

a) le service d'authentification de l'entité homologue est fourni par une combinaison appropriée d'échanges d'authentification obtenus par cryptographie ou protégés, de mécanismes d'échange de mots de passe protégés et de signature;

b) le service d'authentification de l'origine des données peut être fourni par des mécanismes de chiffrement ou de signature;

c) le service de contrôle d'accès est fourni par l'utilisation appropriée de mécanismes spécifiques de contrôle d'accès;

d) le service de confidentialité en mode connexion est fourni par un mécanisme de chiffrement et/ou de contrôle de routage;

e) le service de confidentialité en mode sans connexion est fourni par un mécanisme de chiffrement et/ou de contrôle de routage;

f) le service de confidentialité du flux de données est assuré par un mécanisme de bourrage, combiné à un service de confidentialité au niveau ou au-dessous de la couche réseau, et/ou un mécanisme de contrôle de routage;

g) le service d'intégrité en mode connexion sans reprise est fourni en utilisant un mécanisme d'intégrité des données, parfois combiné à un mécanisme de chiffrement;

h) le service d'intégrité en mode sans connexion est fourni en utilisant un mécanisme d'intégrité des données, parfois combiné àun mécanisme de chiffrement.

7.3.2.2 Les mécanismes du protocole qui effectuent les opérations d'accès au sous-réseau associées à la fourniture du service de réseau OSI entre systèmes d'extrémité, offrent des services via un sous-réseau unique.

La protection d'un sous-réseau imposée par l'administration du sous-réseau sera appliquée comme le prescrivent les protocoles d'accès au sous-réseau, mais sera normalement appliquée avant les fonctions normales de sous-réseau lors de la transmission et après les fonctions normales de sous-réseau lors de la réception.

7.3.2.3 Les mécanismes fournis par le protocole qui effectue les opérations de relais et de routage associées à la fourniture du service de réseau OSI entre systèmes d'extrémité offrent des services via un ou plusieurs réseaux interconnectés.

Ces mécanismes seront appliqués avant les fonctions de relais et de routage lors de la transmission et après les fonctions de relais et de routage lors de la réception. Dans le cas du mécanisme de contrôle de routage, les contraintes de routage appropriées sont obtenues de la SMIB avant que les données ne soient transmises aux fonctions de relais et de routage avec les contraintes de routage nécessaires.

7.3.2.4 Dans la couche réseau, le contrôle d'accès peut avoir plusieurs objectifs. Par exemple, il permet à un système d'extrémité de contrôler l'établissement de connexions de réseau et de rejeter les appels non souhaités. Il permet également à un ou plusieurs sous-réseaux de contrôler l'utilisation des ressources de la couche réseau. Dans certains cas, le contrôle d'accès est associé à l'établissement d'une taxation pour l'utilisation du réseau.

Remarque – L'établissement d'une connexion de réseau peut souvent donner lieu à une taxation imposée par l'administration du sous-réseau. On peut minimiser les coûts en contrôlant l'accès et en choisissant la taxation à l'arrivée ou d'autres paramètres spécifiques au réseau.

7.3.2.5 Les besoins d'un sous-réseau particulier peuvent imposer des mécanismes de contrôle d'accès au protocole qui effectue les opérations d'accès au sous-réseau associées à la fourniture du service de réseau OSI entre systèmes d'extrémité. Lorsque des mécanismes de contrôle d'accès sont fournis par le protocole qui effectue les opérations de relais et de routage associées à la fourniture du service de réseau OSI, entre systèmes d'extrémité, ils peuvent être utilisés à la fois pour contrôler l'accès à des sous-réseaux par des entités relais et pour contrôler l'accès aux systèmes d'extrémité. En clair, la portée de l'isolation du contrôle d'accès est assez grossièrement délimitée, car elle ne fait de distinction qu'entre les entités de la couche réseau.

7.3.2.6 Si le bourrage est combiné à un mécanisme de chiffrement dans la couche réseau (ou à un service de confidentialité de la couche physique), un niveau raisonnable de confidentialité de flux de données peut être atteint.

7.4 *Couche transport*

7.4.1 *Services*

Les services de sécurité qui peuvent être fournis, individuellement ou combinés, dans la couche transport sont:

a) authentification de l'entité homologue;

b) authentification de l'origine des données;

c) contrôle d'accès;

d) confidentialité en mode connexion;

e) confidentialité en mode sans connexion;

f) intégrité en mode connexion avec reprise;

g) intégrité en mode connexion sans reprise;

h) intégrité en mode sans connexion.

7.4.2 *Mécanismes*

Les services de sécurité identifiés sont fournis comme suit:

a) le service d'authentification de l'entité homologue est fourni par une combinaison appropriée d'échanges d'authentification obtenus par cryptographie ou protégés, de mécanisme d'échange de mots de passe protégés et de signature;

b) le service d'authentification de l'origine des données peut être fourni par des mécanismes de chiffrement ou de signature;

c) le service de contrôle d'accès est fourni par l'utilisation appropriée des mécanismes spécifiques de contrôle d'accès;

d) le service de confidentialité en mode connexion est fourni par un mécanisme de chiffrement;

e) le service de confidentialité en mode sans connexion est fourni par un mécanisme de chiffrement;

f) le service d'intégrité en mode connexion avec reprise est fourni en utilisant un mécanisme d'intégrité des données, parfois combiné à un mécanisme de chiffrement;

g) le service d'intégrité en mode connexion sans reprise est fourni en utilisant un mécanisme d'intégrité des données, parfois combiné à un mécanisme de chiffrement;

h) le service d'intégrité en mode sans connexion est fourni en utilisant un mécanisme d'intégrité des données, combiné à un mécanisme de chiffrement.

Les mécanismes de protection fonctionneront de façon que les services de sécurité puissent être appliqués pour des connexions individuelles de transport. La protection sera telle que les connexions individuelles de transport pourront être isolées de toutes les autres connexions de transport.

7.5 *Couche session*

7.5.1 *Services*

Aucun service de sécurité n'est fourni dans la couche session.

7.6 *Couche présentation*

7.6.1 *Services*

Des facilités seront fournies par la couche de présentation pour permettre que les services de sécurité suivants soient fournis par la couche application au processus d'application:

a) confidentialité en mode connexion;

b) confidentialité en mode sans connexion;

c) confidentialité sélective du champ.

Des facilités de la couche présentation peuvent également permettre que les services de sécurité suivants soient fournis par la couche application au processus d'application:

d) confidentialité du flux de données;

e) authentification de l'entité homologue;

f) authentification de l'origine des données;

g) intégrité en mode connexion avec reprise;

h) intégrité en mode connexion sans reprise;

j) intégrité sélective par champ;

k) intégrité en mode sans connexion;

m) intégrité en mode sans connexion sélective par champ;

n) non-répudiation avec preuve de l'origine;

p) non-répudiation avec preuve de la remise.

Remarque – Les facilités fournies par la couche présentation seront celles qui se fondent sur des mécanismes qui ne peuvent fonctionner que sur un codage de la syntaxe de transfert des données et comprendront, par exemple, les fonctionnalités basées sur des techniques cryptographiques.

7.6.2 *Mécanismes*

Pour les services de sécurité suivants, des mécanismes de prise en charge peuvent être situés dans la couche présentation, et s'il en est ainsi, ils peuvent être utilisés en relation avec des mécanismes de sécurité de la couche application pour fournir les services de sécurité de la couche application:

a) le service d'authentification de l'entité homologue peut être pris en charge par des mécanismes de transformation syntaxique (par exemple, le chiffrement);

b) le service d'authentification de l'origine des données peut être pris en charge par des mécanismes de chiffrement ou de signature;

c) le service de confidentialité en mode connexion peut être pris en charge par un mécanisme de chiffrement;

d) le service de confidentialité en mode sans connexion peut être pris en charge par un mécanisme de chiffrement;

e) le service de confidentialité sélective par champ peut être pris en charge par un mécanisme de chiffrement;

f) le service de confidentialité du flux de données peut être pris en charge par un mécanisme de chiffrement;

g) le service d'intégrité en mode connexion avec reprise peut être pris en charge par un mécanisme d'intégrité des données, parfois combiné à un mécanisme de chiffrement;

h) le service d'intégrité en mode connexion sans reprise peut être pris en charge par un mécanisme d'intégrité des données, parfois combiné à un mécanisme de chiffrement;

j) le service d'intégrité en mode connexion sélective par champ peut être pris en charge par un mécanisme d'intégrité des données, parfois combiné à un mécanisme de chiffrement;

k) le service d'intégrité en mode sans connexion peut être pris en charge par un mécanisme d'intégrité des données, parfois combiné à un mécanisme de chiffrement;

m) le service d'intégrité en mode sans connexion sélective par champ peut être pris en charge par un mécanisme d'intégrité des données, parfois combiné à un mécanisme de chiffrement;

n) le service de non-répudiation avec preuve de l'origine peut être pris en charge par une combinaison appropriée de mécanismes d'intégrité des données, de signature et de notarisation;

p) le service de non-répudiation avec preuve de la remise peut être pris en charge par une combinaison appropriée de mécanismes d'intégrité des données, de signature et de notarisation.

Des mécanismes de chiffrement appliqués aux transferts de données, lorsqu'ils sont situés dans les couches supérieures, seront inclus dans la couche présentation.

Certains services de sécurité de la liste ci-dessus peuvent aussi être fournis par des mécanismes de sécurité contenus entièrement dans la couche application.

Seuls les services de sécurité de confidentialité peuvent être entièrement fournis par des mécanismes de sécurité contenus dans la couche présentation.

Les mécanismes de sécurité de la couche présentation fonctionnent en tant que phase finale de la transformation en syntaxe de transfert lors de la transmission, et en tant que phase initiale du processus de transformation lors de la réception.

7.7 *Couche application*

7.7.1 *Services*

La couche application peut fournir un ou plusieurs des services de sécurité suivants, soit individuellement, soit combinés:

a) authentification de l'entité homologue;

b) authentification de l'origine des données;

c) service de contrôle d'accès;

d) confidentialité en mode connexion;

e) confidentialité en mode sans connexion;

f) confidentialité sélective par champ;

g) confidentialité du flux de données;

h) intégrité en mode connexion avec reprise;

j) intégrité en mode connexion sans reprise;

k) intégrité en mode connexion sélective par champ;

m) intégrité en mode sans connexion;

n) intégrité en mode sans connexion sélective par champ;

p) non-répudiation avec preuve de l'origine;

q) non-répudiation avec preuve de la remise.

L'authentification des partenaires prévus de la communication permet la prise en charge des contrôles d'accès aux ressources OSI et non OSI (par exemple fichiers, logiciels, terminaux, imprimantes) dans les systèmes ouverts réels.

Les besoins spécifiques de sécurité dans une instance de communication, y compris la confidentialité, l'intégrité et l'authentification des données, peuvent être déterminés par la gestion de sécurité OSI ou par la gestion de la couche application sur la base des informations de la SMIB, en plus des demandes du processus d'application.

7.7.2 *Mécanismes*

Les services de sécurité de la couche application sont fournis par les mécanismes suivants:

a) le service d'authentification de l'entité homologue peut être fourni en utilisant des informations d'authentification transférées entre les entités d'application, protégées par les mécanismes de chiffrement de la couche présentation ou d'une couche inférieure;

b) le service d'authentification de l'origine des données peut être pris en charge en utilisant les mécanismes de signature ou les mécanismes de chiffrement d'une couche inférieure;

c) le service de contrôle d'accès pour les aspects d'un système ouvert réel qui sont pertinents pour l'OSI, tels que l'aptitude àcommuniquer avec des systèmes spécifiques ou des entités d'application distantes, peut être fourni par une combinaison de mécanismes de contrôle d'accès dans la couche d'application et dans les couches inférieures;

d) le service de confidentialité en mode connexion peut être pris en charge en utilisant un mécanisme de chiffrement d'une couche inférieure;

e) le service de confidentialité en mode sans connexion peut être pris en charge en utilisant un mécanisme de chiffrement d'une couche inférieure;

f) le service de confidentialité sélective par champ peut être pris en charge en utilisant un mécanisme de chiffrement au niveau de la couche présentation;

g) un service limité de confidentialité du flux de données peut être pris en charge en utilisant un mécanisme de bourrage au niveau de la couche application, combiné à un service de confidentialité au niveau d'une couche inférieure;

h) le service d'intégrité en mode connexion avec reprise peut être pris en charge en utilisant un mécanisme d'intégrité des données d'une couche inférieure (parfois combiné à un mécanisme de chiffrement);

j) le service d'intégrité en mode connexion sans reprise peut être pris en charge en utilisant un mécanisme d'intégrité des données d'une couche inférieure (parfois combiné à un mécanisme de chiffrement);

k) le service d'intégrité en mode connexion sélective par champ peut être pris en charge en utilisant un mécanisme d'intégrité des données (parfois combiné à un mécanisme de chiffrement) au niveau de la couche présentation;

m) le service d'intégrité en mode sans connexion peut être pris en charge en utilisant un mécanisme d'intégrité des données d'une couche inférieure (parfois combiné à un mécanisme de chiffrement);

n) le service d'intégrité en mode sans connexion sélective par champ peut être pris en charge en utilisant un mécanisme d'intégrité des données (parfois combiné à un mécanisme de chiffrement) au niveau de la couche présentation;

p) le service de non-répudiation avec preuve de l'origine peut être pris en charge par une combinaison appropriée de mécanisme de signature et de mécanisme d'intégrité des données d'une couche inférieure, éventuellement combiné à l'usage d'un notaire;

q) le service de non-répudiation avec preuve de la remise peut être pris en charge par une combinaison appropriée de mécanisme de signature et de mécanisme d'intégrité des données d'une couche inférieure, éventuellement combiné à l'usage d'un notaire.

Si un mécanisme de notarisation est utilisé pour fournir un service de non-répudiation, il agira comme une tierce partie de confiance. Il peut avoir un enregistrement des unités de données relayées sous leur forme de transfert (c'est-à-dire dans la syntaxe de transfert), afin de résoudre les conflits. Il peut utiliser les services de protection des couches inférieures.

7.7.3 *Services de sécurité non OSI*

Les processus d'application peuvent fournir eux-mêmes l'essentiel des services et utiliser les mêmes types de mécanismes que ceux qui sont décrits dans la présente partie de la Recommandation tels qu'ils sont placés dans les différentes couches de l'architecture. Cette utilisation n'entre pas dans le cadre des définitions des protocoles et des services OSI et de l'architecture OSI, mais elle n'est pas incompatible avec ces définitions.

7.8 *Illustration de la relation entre les services de sécurité et les couches*

Le tableau 2/X.800 montre dans quelles couches du modèle de référence OSI des services de sécurité particuliers peuvent être fournis. Le § 5.2 décrit les services de sécurité. L'annexe B donne les justifications du placement d'un service au niveau d'une couche particulière.

TABLEAU 2/X.800

Illustration de la relation entre les services de sécurité et les couches

Service	Couches						
	1	2	3	4	5	6	7*
Authentification de l'entité homologue	ù	ù	O	O	ù	ù	O
Authentification de l'origine des données	ù	ù	O	O	ù	ù	O
Service de contrôle d'accès	ù	ù	O	O	ù	ù	O
Confidentialité en mode connexion	O	O	O	O	ù	O	O
Confidentialité en mode sans connexion	ù	O	O	O	ù	O	O
Confidentialité sélective par champ	ù	ù	ù	ù	ù	O	O
Confidentialité du flux de données	O	ù	O	ù	ù	ù	O
Intégrité en mode connexion avec reprise	ù	ù	ù	O	ù	ù	O
Intégrité en mode connexion sans reprise	ù	ù	O	O	ù	ù	O
Intégrité en mode connexion sélective par champ	ù	ù	ù	ù	ù	ù	O
Intégrité en mode sans connexion	ù	ù	O	O	ù	ù	O
Intégrité en mode sans connexion sélective par champ	ù	ù	ù	ù	ù	ù	O
Non-répudiation avec preuve de l'origine	ù	ù	ù	ù	ù	ù	O
Non-répudiation avec preuve de la remise	ù	ù	ù	ù	ù	ù	O

O Oui, le service devrait être incorporé dans les normes de la couche en tant qu'option du fournisseur.

ù Service non fourni.

* Il convient de noter que, pour la couche 7, le processus d'application peut fournir lui-même des services de sécurité.

Remarque 1 – Le tableau 2/X.800 ne cherche pas à indiquer que les entrées sont de même importance; au contraire, il y a une variation considérable dans l'importance des entrées des tableaux.

Remarque 2 – Le placement des services de sécurité dans la couche réseau est décrit au § 7.3.2. Le placement des services de sécurité dans la couche réseau affecte de façon significative la nature et le but des services qui seront offerts.

Remarque 3 – La couche présentation contient un certain nombre de facilités de sécurité qui prennent en charge la fourniture de services de sécurité par la couche application.

8 Gestion de sécurité

8.1 *Considérations générales*

8.1.1 La gestion de sécurité OSI traite des aspects de la gestion de sécurité relatifs à l'OSI et à la sécurité de la gestion OSI. Les aspects de gestion de sécurité OSI traitent des opérations qui ne relèvent pas du cadre des instances normales de communication, mais qui sont nécessaires pour prendre en charge et contrôler les aspects de sécurité de ces communications.

Remarque – La disponibilité d'un service de communication est déterminée par la configuration du réseau et/ou par des protocoles de gestion de réseau. Des choix appropriés sont nécessaires pour se protéger contre le déni de service.

8.1.2 L'administration (les administrations) des systèmes ouverts répartis peut imposer un grand nombre de politiques de sécurité et les normes de gestion de sécurité OSI devraient prendre en charge ces politiques. Les entités soumises à une politique de sécurité unique et administrées par une autorité unique, sont parfois rassemblées dans ce que l'on appelle un «domaine de sécurité». Les domaines de sécurité et leurs interactions sont des éléments importants pour de futures extensions de la présente Recommandation.

8.1.3 La gestion de sécurité OSI traite de la gestion des services et mécanismes de sécurité OSI. Ce type de gestion nécessite la répartition d'informations de gestion dans ces services et mécanismes ainsi que la collecte d'informations concernant le fonctionnement de ces services et mécanismes. Ces informations peuvent être, par exemple, la répartition des clés cryptographiques, la détermination de paramètres de sélection de sécurité imposés administrativement, la notification d'événements de sécurité normaux et anormaux (enregistrements d'audits), et l'activation et la désactivation de services. La gestion de sécurité ne s'occupe pas de faire passer des informations concernant la sécurité dans les protocoles qui font appel à des services de sécurité spécifiques (par exemple, dans les paramètres de demandes de connexion).

8.1.4 La base d'informations de gestion de sécurité (SMIB) est l'ensemble conceptuel des informations de sécurité dont ont besoin les systèmes ouverts. Ce concept ne suppose rien quant à la forme et à la réalisation du stockage des informations. Cependant, chaque système d'extrémité doit contenir les informations locales nécessaires pour lui permettre d'appliquer une politique de sécurité appropriée. La SMIB est une base d'informations répartie dans la mesure où il est nécessaire d'appliquer une politique de sécurité cohérente dans un groupement (logique ou physique) de systèmes d'extrémité. Dans la pratique, des parties de la SMIB peuvent ou non être intégrées à la MIB.

Remarque – La SMIB peut donner lieu à de nombreuses réalisations, par exemple:

a) un tableau de données;

b) un fichier;

c) des données ou des règles intégrées au logiciel ou au matériel du système ouvert réel.

8.1.5 Les protocoles de gestion, surtout les protocoles de gestion de sécurité, et les voies de communication acheminant les informations de gestion, sont potentiellement vulnérables. Il faut donc veiller tout particulièrement à protéger les protocoles et les informations de gestion de façon à ne pas affaiblir la protection de sécurité prévue pour les instances de communication habituelles.

8.1.6 La gestion de sécurité peut nécessiter l'échange d'informations de sécurité entre diverses administrations de système pour que la SMIB puisse être établie ou étendue. Dans certains cas, les informations relatives à la sécurité seront transmises par des voies de communication non OSI, et les administrateurs de systèmes locaux mettront à jour la SMIB selon des méthodes non normalisées par l'OSI. Dans d'autres cas, il peut être souhaitable d'échanger ces informations par une voie de communication OSI; les informations seront alors transmises entre deux applications de gestion de sécurité fonctionnant dans les systèmes ouverts réels. L'application de la gestion de sécurité utilisera les informations communiquées pour mettre à jour la SMIB. Cette mise à jour de la SMIB peut nécessiter l'autorisation préalable de l'administrateur approprié de la sécurité.

8.1.7 Des protocoles d'application seront définis pour l'échange d'informations relatives à la sécurité par des voies de communication OSI.

8.2 *Catégories de gestion de sécurité OSI*

Il y a trois catégories d'activité de gestion de sécurité OSI:

a) gestion de sécurité-système;

b) gestion de services de sécurité;

c) gestion de mécanismes de sécurité.

Il faut, en outre, prendre en considération la sécurité de la gestion OSI (voir le § 8.2.4). Les fonctions clés assurées par ces catégories de gestion de sécurité sont résumées ci-dessous.

8.2.1 *Gestion de sécurité-système*

La gestion de sécurité-système traite de la gestion des aspects de sécurité de l'environnement OSI en général. La liste suivante est un exemple de liste d'activités entrant dans cette catégorie de gestion de sécurité:

a) gestion globale de la politique de sécurité, comprenant les mises à jour et le maintien de la cohérence;

b) interaction avec d'autres fonctions de gestion OSI;

c) interaction avec la gestion de services de sécurité et la gestion de mécanismes de sécurité;

d) gestion de traitement d'événements (voir le § 8.3.1);

e) gestion d'audit de sécurité (voir le § 8.3.2);

f) gestion de reprise de sécurité (voir le § 8.3.3).

8.2.2 *Gestion de services de sécurité*

La gestion de services de sécurité traite de la gestion de services de sécurité particuliers. La liste suivante est un exemple de liste d'activités pouvant être effectuées lors de la gestion d'un service de sécurité particulier:

a) détermination et affectation de la protection de sécurité cible pour le service;

b) affectation et maintien de règles de sélection (lorsqu'il existe d'autres possibilités) du mécanisme de sécurité spécifique à utiliser pour fournir le service de sécurité demandé;

c) négociation (locale et à distance) des mécanismes de sécurité disponibles nécessitant un accord de gestion préalable;

d) application de mécanismes de sécurité spécifiques via la fonction appropriée de gestion de mécanismes de sécurité, par exemple pour la fourniture de services de sécurité imposés administrativement;

e) interaction avec d'autres fonctions de gestion de services de sécurité et de mécanismes de sécurité.

8.2.3 *Gestion de mécanismes de sécurité*

La gestion de mécanismes de sécurité traite de la gestion de mécanismes de sécurité particuliers. La liste suivante est un exemple de liste de fonctions de gestion de mécanismes de sécurité, mais elle n'est pas exhaustive:

a) gestion de clés;

b) gestion de chiffrement;

c) gestion de signature numérique;

d) gestion de contrôle d'accès;

e) gestion d'intégrité des données;

f) gestion d'authentification;

g) gestion de bourrage;

h) gestion de contrôle du routage;

j) gestion de notarisation.

Chacune des fonctions de gestion de mécanismes de sécurité figurant dans cette liste est présentée plus en détail au § 8.4.

8.2.4 *Sécurité de la gestion OSI*

La sécurité de toutes les fonctions de gestion OSI et de la communication des informations de gestion OSI sont des parties importantes de la sécurité OSI. Cette catégorie de gestion de la sécurité repose sur des choix appropriés de services et de mécanismes de sécurité OSI répertoriés pour garantir que les protocoles et les informations de gestion OSI sont protégés de façon adéquate (voir le § 8.1.5). Par exemple, les communications entre les entités de gestion impliquant la base d'informations de gestion nécessiteront généralement une certaine forme de protection.

8.3 *Activités spécifiques de gestion de sécurité-système*

8.3.1 *Gestion de traitement d'événements*

Les aspects de gestion de traitement d'événements visibles dans l'OSI sont la notification à distance de tentatives apparentes de violer la sécuritésystème et la modification des seuils utilisés pour déclencher la notification des événements.

8.3.2 *Gestion d'audit de sécurité*

La gestion d'audit de sécurité peut comprendre:

a) le choix d'événements à enregistrer et/ou à collecter à distance;

b) la validation et l'invalidation de l'enregistrement de journal d'audit d'événements choisis;

c) la collecte à distance d'enregistrements d'audit choisis;

d) la préparation de rapports d'audit de sécurité.

8.3.3 *Gestion de reprise de sécurité*

La gestion de reprise de sécurité peut comprendre:

a) le maintien des règles utilisées pour réagir contre les violations de sécurité réelles ou suspectées;

b) la notification à distance de violations apparentes de la sécurité-système;

c) les interactions de l'administrateur de sécurité.

8.4 *Fonctions de gestion de mécanismes de sécurité*

8.4.1 *Gestion de clés*

La gestion de clés peut comprendre:

a) la génération de clés appropriées à intervalles dépendant du niveau de sécurité requis;

b) la détermination, conformément aux besoins de contrôle d'accès, des entités qui devraient recevoir une copie de chaque clé;

c) la mise à disposition ou la répartition des clés de façon sûre aux instances d'entité dans des systèmes ouverts réels.

Il est entendu que certaines fonctions de gestion de clés seront effectuées à l'extérieur de l'environnement OSI. Ces fonctions comprennent la répartition physique des clés par des moyens de confiance.

L'échange de clés de travail à utiliser au cours d'une association est une fonction de protocole ordinaire de couche. Le choix de clés de travail peut également être fait en accédant à un centre de répartition des clés ou par répartition préalable via les protocoles de gestion.

8.4.2 *Gestion de chiffrement*

La gestion de chiffrement peut comprendre:

a) l'interaction avec la gestion des clés;

b) l'établissement de paramètres cryptographiques;

c) la synchronisation cryptographique.

L'existence d'un mécanisme de chiffrement implique l'utilisation de la gestion de clés et de méthodes communes pour faire référence à des algorithmes cryptographiques.

Le degré de discrimination de la protection apportée par le chiffrement est déterminé par les entités qui, dans l'environnement OSI, ont des clés indépendantes. Ceci est à son tour déterminé, en général, par l'architecture de sécurité et, plus spécifiquement, par le mécanisme de gestion de clés.

Une référence commune pour les algorithmes cryptographiques peut être obtenue moyennant l'utilisation d'un registre pour les algorithmes cryptographiques ou par accord préalable entre entités.

8.4.3 *Gestion de signature numérique*

La gestion de signature numérique peut comprendre:

a) l'interaction avec la gestion des clés;

b) l'établissement de paramètres et d'algorithmes cryptographiques;

c) l'utilisation d'un protocole entre les entités communicantes et, éventuellement, un tiers.

Remarque – Il existe, en général, de grandes similitudes entre la gestion de signature numérique et la gestion de chiffrement.

8.4.4 *Gestion de contrôle d'accès*

La gestion de contrôle d'accès peut comprendre la répartition des attributs de sécurité (y compris les mots de passe) ou les mises à jour de listes de contrôle d'accès ou de liste de capacités. Elle peut également comprendre l'utilisation d'un protocole entre les entités communicantes et d'autres entités fournissant des services de contrôle d'accès.

8.4.5 *Gestion d'intégrité des données*

La gestion d'intégrité des données peut comprendre:

a) l'interaction avec la gestion des clés;

b) l'établissement de paramètres et d'algorithmes cryptographiques;

c) l'utilisation d'un protocole entre les entités communicantes.

Remarque – Lorsqu'on utilise des techniques cryptographiques pour l'intégrité des données, il existe de grandes similitudes entre la gestion d'intégrité des données et la gestion de chiffrement.

8.4.6 *Gestion d'authentification*

La gestion d'authentification peut comprendre la répartition d'informations descriptives, de mots de passe ou de clés (à l'aide de la gestion des clés) entre les entités qui doivent effectuer une authentification. Elle peut également comprendre l'utilisation d'un protocole entre les entités communicantes et d'autres entités fournissant des services d'authentification.

8.4.7 *Gestion de bourrage*

La gestion de bourrage peut comprendre le maintien des règles à utiliser pour le bourrage. Par exemple, cela peut comprendre:

a) des débits de données spécifiés au préalable;

b) la spécification de débits aléatoires;

c) la spécification de caractéristiques de message telles que la longueur;

d) l'adaptation de la spécification, éventuellement en fonction de l'heure et/ou du calendrier.

8.4.8 *Gestion de contrôle de routage*

La gestion de contrôle de routage peut comprendre la définition de liaisons ou sous-réseaux que l'on considère soit comme sûrs, soit comme de confiance par rapport à des critères particuliers.

8.4.9 *Gestion de notarisation*

La gestion de notarisation peut comprendre:

a) la répartition des informations relatives aux notaires;

b) l'utilisation d'un protocole entre un notaire et les entités communicantes;

c) l'interaction avec les notaires.

ANNEXE A

Informations de base sur la sécurité dans l'OSI

(La présente annexe ne fait pas partie intégrante de la Recommandation)

A.1 *Informations de base*

La présente annexe fournit:

a) des informations sur la sécurité OSI afin de placer la présente Recommandation dans une certaine perspective;

b) des bases relatives aux incidences du point de vue de l'architecture, des diverses caractéristiques et exigences de sécurité.

La sécurité dans un environnement OSI n'est qu'un aspect de la sécurité du traitement des données/des communications de données. Pour être efficaces, les mesures de protection utilisées dans un environnement OSI nécessitent la mise en œuvre de moyens sortant du cadre de l'OSI. Par exemple, des informations passant entre des systèmes peuvent être chiffrées, mais si aucune restriction physique de sécurité n'est imposée à l'accès aux systèmes eux-mêmes, le chiffrement peut être fait en vain. L'OSI ne s'occupe que de l'interconnexion de systèmes. Pour que les mesures de sécurité OSI soient efficaces, elles doivent être associées à des mesures qui n'entrent pas dans le cadre de l'OSI.

A.2 *Besoins de sécurité*

A.2.1 *Qu'entend-on par sécurité?*

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.

A.2.2 *Motivation pour la sécurité dans les systèmes ouverts*

Le CCITT a reconnu la nécessité d'une série de normes visant à améliorer la sécurité dans l'architecture d'interconnexion des systèmes ouverts. Cette nécessité vient de:

a) la dépendance croissante de la société vis-à-vis des ordinateurs auxquels on a accès, ou qui sont liés par des moyens de communications de données et qui nécessitent une protection contre diverses menaces;

b) l'apparition, dans plusieurs pays, d'une législation sur la «protection des données» qui oblige les fournisseurs à démontrer l'intégrité de leur système et la manière de respecter la vie privée;

c) le souhait de diverses organisations d'utiliser les normes OSI, améliorées selon les besoins, pour des systèmes sûrs existants et à venir.

A.2.3 *Que doit-on protéger?*

En général, les éléments suivants peuvent nécessiter une protection:

a) informations et données (y compris le logiciel et les données passives relatives aux mesures de sécurité telles que les mots de passe);

b) services de communication et de traitement des données;

c) équipements et facilités.

A.2.4 *Menaces*

Les menaces envers un système de communication de données comprennent les éléments suivants:

a) destruction d'informations et/ou d'autres ressources;

b) corruption ou modification d'informations;

c) vol, suppression ou perte d'informations et/ou d'autres ressources;

d) divulgation d'informations;

e) interruption de services.

Les menaces peuvent être classées en menaces accidentelles ou menaces intentionnelles et elles peuvent être actives ou passives.

A.2.4.1 *Menaces accidentelles*

Les menaces accidentelles sont celles 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.

A.2.4.2 *Menaces intentionnelles*

Les menaces intentionnelles peuvent 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».

A.2.4.3 *Menaces passives*

Les menaces passives sont celles qui, si elles se concrétisent, ne produiraient aucune modification d'informations contenues dans le(s) système(s) et avec lesquelles ni le fonctionnement, ni l'état du système ne changent. L'utilisation de branchements clandestins passifs pour observer des informations transmises via une ligne de communication est une concrétisation d'une menace passive.

A.2.4.4 *Menaces actives*

Les menaces actives envers un système comprennent l'altération d'informations contenues dans ce système, ou des modifications de l'état ou du fonctionnement du système. Une modification malveillante des tables de routage d'un système par un utilisateur non autorisé est un exemple de menace active.

A.2.5 *Quelques types d'attaque spécifiques*

Les paragraphes suivants passent brièvement en revue quelques-unes des attaques particulièrement intéressantes dans un environnement de traitement de données/de communication de données. Dans ces paragraphes, apparaissent les termes «autorisé» et «non autorisé». «Autorisation» signifie l'«octroi de droits». Les deux éléments qu'implique cette définition sont les suivants: les droits sont des droits d'effectuer certaines activités (telles que l'accès aux données); ils ont été accordés à une entité, un opérateur humain ou un processus. Le comportement autorisé est alors l'exécution de ces activités pour lesquelles des droits ont été octroyés (et non abrogés). Le § A.3.3.1 donne plus de détails sur le concept d'autorisation.

A.2.5.1 *Usurpation de l'identité*

L'usurpation de l'identité est le procédé par lequel une entité se fait passer pour une autre. Elle est généralement utilisée avec d'autres formes d'attaque active, surtout le fait de répéter la modification des messages. Par exemple, des séquences d'authentification peuvent être capturées et répétées après qu'une séquence d'authentification correcte a eu lieu. Une entité autorisée ayant peu de privilèges peut utiliser une usurpation d'identité pour obtenir des privilèges supplémentaires en usurpant l'identité d'une entité qui a ces privilèges.

A.2.5.2 *Le fait de répéter*

Le fait de répéter survient lorsqu'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).

A.2.5.3 *Modification des messages*

La modification d'un message a lieu lorsque le contenu d'une transmission de données est modifié sans que cela soit détecté et produit un effet non autorisé, comme lorsque, par exemple, un message «Autoriser 'John Smith' à lire le fichier confidentiel 'comptes'» est modifié en «Autoriser 'Fred Brown' à lire le fichier confidentiel 'comptes'».

A.2.5.4 *Déni de service*

Le déni de service a lieu lorsqu'une entité ne remplit pas sa propre fonction ou agit de façon qui empêche d'autres entités de remplir leurs propres fonctions. L'attaque peut être générale comme lorsqu'une entité supprime tous les messages; ou bien, l'attaque peut avoir un but spécifique, comme lorsqu'une entité supprime tous les messages envoyés à un destinataire particulier (le service d'audit de sécurité, par exemple). L'attaque peut comprendre la suppression du trafic telle qu'elle est décrite dans cet exemple, ou bien elle peut générer un trafic supplémentaire. Il est également possible de générer des messages afin de désorganiser le fonctionnement du réseau, surtout si ce réseau compte des entités relais qui prennent des décisions de routage fondées sur des rapports d'état reçus d'autres entités relais.

A.2.5.5 *Attaques de l'intérieur*

Des attaques de l'intérieur se produisent lorsque des utilisateurs légitimes d'un système se comportent de façon non attendue ou, non autorisée. La plupart des délits informatiques connus ont comporté des attaques de l'intérieur qui ont compromis la sécurité du système. Les méthodes de protection qui peuvent être utilisées contre des attaques de l'intérieur comprennent:

a) un contrôle attentif du personnel;

b) un examen minutieux du matériel, du logiciel, de la politique de sécurité et des configurations de système afin qu'il y ait un certain degré de garantie de bon fonctionnement (appelé fonctionnalité de confiance);

c) des journaux d'audit pour augmenter la probabilité de détecter ces attaques.

A.2.5.6 *Attaques de l'extérieur*

Des attaques de l'extérieur peuvent utiliser des techniques telles que:

a) branchement clandestin (actif et passif);

b) interception d'émission;

c) usurpation d'identité en utilisateurs autorisés du système ou en composant du système;

d) court-circuit des mécanismes d'authentification ou de contrôle d'accès.

A.2.5.7 *Trappes*

Lorsqu'une entité d'un système est modifiée pour permettre à un attaquant de produire un effet non autorisé sur demande ou lors d'un événement d'une séquence d'événements prédéterminés, le résultat est appelé trappe. Par exemple, une validation de mot de passe pourrait être modifiée de façon à valider également le mot de passe d'un attaquant, en plus de son effet normal.

A.2.5.8 *Cheval de Troie*

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».

A.2.6 *Evaluation des menaces, risques et contre-mesures*

Les caractéristiques de sécurité augmentent généralement le coût d'un système et peuvent le rendre plus difficile à utiliser. Avant de concevoir un système sûr, il convient donc d'identifier les menaces spécifiques contre lesquelles une protection est nécessaire. C'est ce que l'on appelle «évaluation de la menace». Un système est vulnérable de plusieurs façons, mais seules certaines de ces façons sont exploitables parce que l'attaquant n'a pas l'occasion d'intervenir, ou parce que le résultat ne justifie ni l'effort, ni le risque de se faire détecter. Bien que le détail de l'évaluation des menaces ne relève pas du domaine d'application de la présente annexe, cette évaluation porte en gros sur:

a) l'identification des vulnérabilités du système;

b) l'analyse de la probabilité des menaces visant à exploiter ces vulnérabilités;

c) l'évaluation des conséquences qu'aurait la réalisation de chaque menace;

d) l'évaluation du coût de chaque attaque;

e) l'établissement du prix de revient d'éventuelles contre-mesures;

f) le choix des mécanismes de sécurité qui sont justifiés (éventuellement en utilisant une analyse du rapport avantage-coût).

Des mesures non techniques, telles que l'assurance, peuvent être des solutions de rechange rentables aux mesures de sécurité technique. Une sécurité technique parfaite, comme une sécurité physique parfaite, est impossible. L'objectif devrait donc être de rendre le coût d'une attaque suffisamment élevé pour ramener le risque à des niveaux acceptables.

A.3 *Politique de sécurité*

Le présent paragraphe traite de politique de sécurité: la nécessité d'une politique de sécurité correctement définie; son rôle; les méthodes politiques utilisées et les améliorations à apporter dans des situations spécifiques. Ces concepts sont ensuite appliqués aux systèmes de communication.

A.3.1 *Nécessité et but d'une politique de sécurité*

L'ensemble du domaine de sécurité est à la fois complexe et d'une portée considérable. Toute analyse suffisamment complète donnera une pléthore de détails. Une politique de sécurité appropriée devrait concentrer l'attention sur les aspects d'une situation que le niveau le plus élevé de l'autorité juge digne d'attention. Pour l'essentiel, une politique de sécurité précise, en termes généraux, ce qui est permis et ce qui ne l'est pas, dans le domaine de la sécurité lors du fonctionnement général du système en question. Une politique de sécurité n'est généralement pas spécifique: elle suggère ce qui présente une importance capitale sans dire précisément comment les résultats souhaités doivent être obtenus. Une politique de sécurité fixe le niveau maximal d'une spécification de sécurité.

A.3.2 *Ce qu'implique une définition de politique de sécurité: le processus d'affinement*

Une politique de sécurité étant générale, on ne voit pas bien comment elle pourrait être appliquée à une application donnée. Souvent, la meilleure façon de procéder consiste à affiner progressivement la politique de sécurité en ajoutant de plus en plus de détails à partir de l'application à chaque niveau. Savoir ce que ces détails devraient être nécessite une étude détaillée du domaine d'application à la lumière de la politique de sécurité. Cet examen devrait définir les problèmes qui se posent lorsqu'on essaie d'imposer les conditions de la politique de sécurité à l'application. Le processus d'affinement permettra de redéfinir la politique de sécurité générale en termes très précis directement tirés de l'application. Cette politique une fois redéfinie facilitera la détermination des détails de la mise en œuvre.

A.3.3 *Composantes de la politique de sécurité*

Les politiques de sécurité existantes comportent deux aspects. Ils dépendent tous deux du concept de comportement autorisé.

A.3.3.1 *Autorisation*

Les menaces dont il a déjà été question impliquent toutes la notion de comportement autorisé et non autorisé. La déclaration définissant ce qui constitue une autorisation se concrétise dans la politique de sécurité. Une politique de sécurité générique pourrait dire: «l'information ne peut pas être donnée aux personnes n'ayant pas l'autorisation appropriée; ces personnes ne peuvent avoir accès, ou ne peuvent pas intervenir sur cette information, ni utiliser une ressource». La nature de l'autorisation est ce qui distingue les différentes politiques de sécurité. Les politiques de sécurité peuvent être divisées en deux composantes suivant la nature de l'autorisation qu'elles comportent, politiques fondées sur des règles, ou politiques fondées sur l'identité. Les premières utilisent des règles fondées sur un petit nombre d'attributs généraux ou de classes de sensibilité qui sont universellement appliquées. Les secondes comprennent des critères d'autorisation fondés sur des attributs spécifiques individualisés. Certains attributs sont supposés être associés en permanence à l'entité à laquelle ils s'appliquent; d'autres peuvent être des possessions (telles que des capacités) qui peuvent être transmises à d'autres entités. On peut également établir une distinction entre le service d'autorisation imposé administrativement et le service d'autorisation choisi de façon dynamique. Une politique de sécurité déterminera les éléments de la sécurité-système qui sont toujours appliqués et en vigueur (par exemple, les éventuels composants de la politique de sécurité fondée sur des règles et ceux de la politique de sécurité fondée sur l'identité) et ceux que l'utilisateur peut choisir d'utiliser à sa convenance.

A.3.3.2 *Politique de sécurité fondée sur l'identité*

Dans les politiques de sécurité, l'aspect «fondées sur l'identité» correspond en partie au concept de sécurité connu sous le nom de «besoin de connaître». Le but est de filtrer l'accès aux données ou aux ressources. Il y a deux façons principales de mettre en œuvre les politiques fondées sur l'identité selon que les informations sur les droits d'accès sont détenues par celui qui y a accès ou que ces informations font partie des données auxquelles on a accès. Dans le premier cas, par exemple, des privilèges ou capacités sont accordés aux utilisateurs et utilisés par des processus agissant en leur nom. Dans le second, des listes de contrôles d'accès (ACL) peuvent, par exemple, être utilisées. Dans les deux cas, la taille des données (allant d'un fichier complet à un élément de données) qui peut être nommée dans une capacité ou qui transporte sa propre ACL, peut être extrêmement variable.

A.3.3.3 *Politique de sécurité fondée sur des règles*

Dans une politique de sécurité fondée sur des règles, l'autorisation repose généralement sur la sensibilité. Dans un système sûr, les données et/ou les ressources devraient être marquées avec des étiquettes de sécurité. Les processus agissant au nom d'utilisateurs humains peuvent acquérir l'étiquette de sécurité correspondant à leurs créateurs.

A.3.4 *Politique de sécurité, communications et étiquettes*

Le concept d'étiquetage est important dans un environnement de communication de données. Les étiquettes portant des attributs jouent toute une gamme de rôles. Les données transférées au cours de la communication, les processus et entités agissant en initiateur ou répondeur, les voies de communication utilisées peuvent tous être étiquetés, d'une façon ou d'une autre, par leurs attributs. Les politiques de sécurité doivent indiquer comment utiliser

chaque attribut pour assurer la sécurité requise. Une négociation peut s'avérer nécessaire pour établir ce que certains attributs signifient exactement pour la sécurité. Lorsque des étiquettes de sécurité sont liées à la fois aux processus accédant aux données et aux données auxquelles ils accèdent, les informations supplémentaires nécessaires à un contrôle d'accès fondé sur l'identité devraient être incluses dans les étiquettes pertinentes. Lorsqu'une politique de sécurité est fondée sur l'identité de l'utilisateur qui accède aux données, soit directement, soit par un processus, les étiquettes de sécurité devraient alors inclure des informations sur l'identité de l'utilisateur. Les règles concernant des étiquettes particulières devraient être exprimées dans une politique de sécurité et incluses dans la base d'informations de gestion de la sécurité (SMIB) et/ou négociées avec les systèmes d'extrémité, selon les besoins. L'étiquette peut être accompagnée d'attributs qualifiant sa sensibilité, spécifier les précautions concernant le traitement et la distribution, introduire des contraintes de temps et de mise à disposition et énoncer des exigences spécifiques au système d'extrémité.

A.3.4.1 *Etiquettes de processus*

Dans l'authentification, l'identification complète des processus ou entités agissant comme initiateur ou répondeur dans une instance de communication, ainsi que tous les attributs appropriés revêtent une importance fondamentale. Les SMIB contiendront donc suffisamment d'informations sur les attributs qui sont importants pour toute politique imposée par une Administration.

A.3.4.2 *Etiquettes de données*

Les données transférées au cours des instances de communication sont étroitement liées à leur étiquette (cette liaison est significative et, pour certaines instances de politiques de sécurité fondées sur des règles, il est prescrit de faire de l'étiquette une partie spéciale des données avant qu'elles soient remises à l'application). Des techniques permettant de préserver l'intégrité des données maintiendront également l'exactitude de l'étiquette et son lien avec les données. Ces attributs peuvent être utilisés par les fonctions de contrôle de routage dans la couche liaison de données du modèle de référence de base OSI.

A.4 *Mécanismes de sécurité*

Une politique de sécurité peut être mise en œuvre à l'aide de divers mécanismes; suivant les objectifs de la politique de sécurité et les mécanismes utilisés, chaque mécanisme peut être utilisé seul ou combiné à d'autres mécanismes. En général, un mécanisme appartiendra à l'une des trois classes suivantes (qui se chevauchent):

a) prévention;

b) détection;

c) reprise.

Les mécanismes de sécurité appropriés pour un environnement de communication de données sont présentés ci-dessous.

A.4.1 *Techniques cryptographiques et chiffrement*

La cryptographie est à la base de nombreux services et mécanismes de sécurité. Des fonctions cryptographiques peuvent être utilisées dans le chiffrement, le déchiffrement, l'intégrité des données, les échanges d'authentification, le stockage et de la vérification des mots de passe, etc., pour aider à obtenir la confidentialité, l'intégrité et/ou l'authentification. Le chiffrement, utilisé dans la confidentialité, transforme les données sensibles (c'est-à-dire les données à protéger) en données moins sensibles. Dans l'intégrité ou l'authentification, les techniques cryptographiques sont utilisées pour traiter des fonctions non falsifiables.

Le chiffrement s'effectue au départ sur un texte en clair pour produire un texte chiffré. Le résultat du déchiffrement est soit un texte en clair, soit un texte chiffré sous une forme quelconque. Il est possible d'utiliser un texte en clair pour un traitement informatique d'ordre général, le contenu sémantique du texte étant accessible; il n'est pas possible de traiter un texte chiffré, son contenu sémantique étant caché, sauf de façons très spécifiques (par exemple: déchiffrement ou correspondance exacte). Le chiffrement est parfois volontairement irréversible (par exemple, par troncature ou perte des données) lorsqu'on désire que le texte en clair d'origine, tels que les mots de passe, ne soit jamais retrouvé.

Les fonctions cryptographiques utilisent des cryptovariables et fonctionnent sur des champs d'unité de données, des unités de données et/ou des flux d'unités de données. Deux de ces cryptovariables sont la clé qui guide les transformations spécifiques et la variable d'initialisation, requise dans certains protocoles cryptographiques pour préserver le caractère aléatoire apparent du texte chiffré. La clé doit généralement rester confidentielle et la fonction cryptographique ainsi que la variable d'initialisation peuvent augmenter les délais de transmission et la consommation de bande passante. Cela complique les ajouts cryptographiques «transparents» ou «parasites» sur les systèmes existants.

Les variables cryptographiques peuvent être symétriques ou asymétriques pour le chiffrement et le déchiffrement. Les clés utilisées dans les algorithmes asymétriques sont reliées mathématiquement; on ne peut pas calculer une clé à partir d'une autre. Ces algorithmes sont parfois appelés algorithmes «à clés publiques», car une clé peut être rendue publique tandis que l'autre peut être gardée secrète.

Le texte chiffré peut être décrypté lorsqu'il est possible, par l'informatique, de retrouver le texte en clair sans connaître la clé. Cela peut arriver si une fonction cryptographique faible ou défectueuse est utilisée. Les interceptions et les analyses de trafic peuvent conduire à des attaques sur le cryptosystème y compris l'insertion de message/de champ, la suppression et le changement, le fait de répéter un texte chiffré préalablement valide et l'usurpation d'identité.

Des protocoles cryptographiques sont donc conçus pour résister aux attaques et parfois, à l'analyse de trafic. Une mesure spécifique contre l'analyse de trafic, la «confidentialité du flux de données», vise à cacher la présence ou l'absence de données et ses caractéristiques. Si le texte chiffré est acheminé par des relais, l'adresse doit être en clair au niveau des relais et des passerelles. Si les données ne sont chiffrées que sur chaque liaison et déchiffrées (donc vulnérables) au niveau des relais ou de la passerelle, on dira que l'architecture utilise un «chiffrement liaison par liaison». Si seule l'adresse (et les données de contrôle similaires) sont en clair dans le relais ou la passerelle, on dira que l'architecture utilise un «chiffrement de bout en bout». Le chiffrement de bout en bout est plus souhaitable du point de vue de la sécurité, mais il est nettement plus complexe du point de vue de l'architecture, surtout si la répartition des clés électroniques (une fonction de gestion de clés) est incluse en même temps. On peut combiner le chiffrement liaison par liaison et le chiffrement de bout en bout pour atteindre plusieurs objectifs de sécurité. L'intégrité des données est souvent réalisée en calculant une valeur de contrôle cryptographique. La valeur de contrôle peut être dérivée en une ou plusieurs étapes; c'est une fonction mathématique des cryptovariables et des données. Ces valeurs de contrôle sont associées aux données qui doivent être protégées. Les valeurs de contrôle cryptographiques sont parfois appelées codes de détection de manipulation.

Les techniques cryptographiques peuvent fournir, ou aider à fournir, une protection contre:

a) l'observation et/ou la modification du train de messages;

b) l'analyse de trafic;

c) la répudiation;

d) la falsification;

e) la connexion non autorisée;

f) la modification des messages.

A.4.2 *Aspects de la gestion des clés*

L'utilisation d'algorithmes cryptographiques implique une gestion des clés. La gestion des clés englobe la production, la répartition et le contrôle des clés cryptographiques. Le choix d'une méthode de gestion des clés est fondée sur l'évaluation, par les participants, de l'environnement dans lequel elle doit être utilisée. Les éléments de cet environnement comprennent les menaces contre lesquelles il faut se protéger (à la fois internes et externes à l'organisation), les technologies utilisées, l'architecture et l'emplacement des services cryptographiques fournis, la structure physique et l'emplacement des fournisseurs des services cryptographiques.

Les points à prendre en compte dans la gestion de clés sont:

a) l'utilisation, implicite ou explicite, d'une «durée de vie» fondée sur la durée, l'utilisation ou autres critères, pour chaque clé définie;

b) l'identification correcte des clés suivant leur fonction, de sorte que leur utilisation puisse être réservée uniquement à leur fonction; par exemple, les clés prévues pour être utilisées pour un service de confidentialité ne devraient pas être utilisées pour un service d'intégrité et vice versa;

c) des considérations non OSI, telles que la répartition physique des clés et leur archivage.

Les points à prendre en compte dans la gestion des clés, dans le cas d'algorithmes de clés symétriques, sont:

a) l'utilisation d'un service de confidentialité dans le protocole de gestion des clés, pour acheminer les clés;

b) l'utilisation d'une hiérarchie des clés. Différentes situations pourraient être autorisées:

   1) des hiérarchies de clés «plates», n'utilisant que des clés de chiffrement de données, choisies implicitement ou explicitement dans un jeu de clés, d'après l'identité de la clé ou par un index,

   2) des hiérarchies de clés multicouches,

   3) des clés de chiffrement de clés ne devraient jamais être utilisées pour protéger des données et des clés de chiffrement de données ne devraient jamais être utilisées pour protéger des chiffrements de clés;

c) la division des responsabilités, de telle sorte que personne ne possède une copie complète d'une clé importante.

Les points à prendre en compte dans la gestion des clés, dans le cas d'algorithmes de clés asymétriques, sont:

a) l'utilisation d'un service de confidentialité dans le protocole de gestion des clés, pour acheminer les clés privées;

b) l'utilisation d'un service d'intégrité, ou d'un service de nonrépudiation avec preuve de l'origine, dans le protocole de gestion de clés, pour acheminer les clés publiques. Ces services peuvent être fournis à l'aide des algorithmes cryptographiques symétriques et/ou asymétriques.

A.4.3 *Mécanismes de signature numérique*

Le terme de «signature numérique» désigne une technique particulière qui peut être utilisée pour fournir des services de sécurité tels que la non-répudiation et l'authentification. Les mécanismes de signature numérique nécessitent l'utilisation d'algorithmes cryptographiques asymétriques. La caractéristique essentielle du mécanisme de signature numérique est que l'unité de données signée ne peut pas être créée sans utiliser la clé privée. Cela signifie que:

a) l'unité de données signée ne peut être créée que par le détenteur de la clé privée;

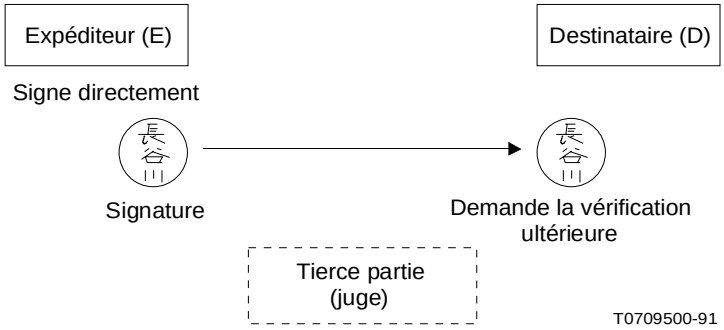
b) le destinataire ne peut pas créer l'unité de données signée.

Par conséquent, en n'utilisant que des informations publiques, il est possible d'identifier sans ambiguïté le signataire d'une unité de données comme étant le détenteur de la clé privée. En cas de litige ultérieur entre les participants, il est donc possible de prouver l'identité du signataire d'une unité de données à une tierce partie fiable qui sera appelée à juger de l'authenticité de l'unité de données signée. Ce type de signature numérique s'appelle schéma de signature directe (voir la figure A-1/X.800). Dans d'autres cas, la propriété présentée en c) ci-dessous peut, en plus, être nécessaire:

c) l'expéditeur ne peut pas nier avoir envoyé l'unité de données signée.

Dans ce cas, une tierce partie fiable (arbitre) prouve au destinataire la source et l'intégrité des informations. Ce type de signature numérique est parfois appelé schéma de signature arbitré (voir la figure A-2/X.800).

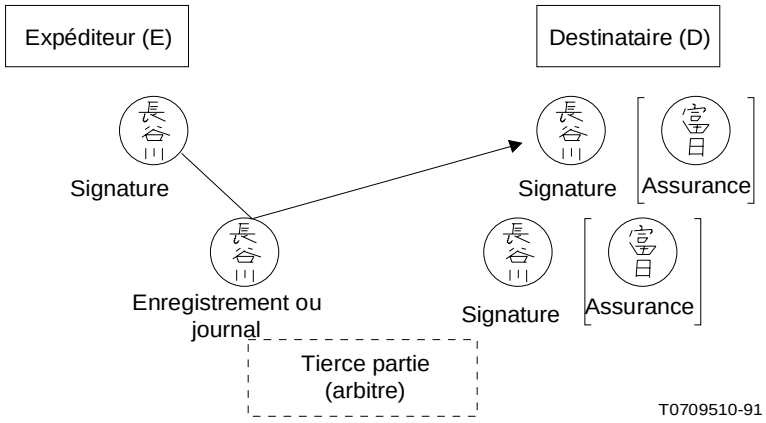
Remarque – L'expéditeur peut demander que le destinataire ne puisse pas nier, par la suite, avoir reçu l'unité de données signée. Ceci est réalisable avec un service de non-répudiation avec preuve de la remise, au moyen d'une combinaison appropriée des mécanismes de signature numérique, d'intégrité de données et de notarisation.



Remarque — Vérifie la signature lorsqu'un conflit naît entre les participants (E peut être parjure ou D peut être parjure).

FIGURE A-1/X.800

Schéma de signature directe



Remarque — Une tierce partie authentifie la source et donne la garantie (c'est-à-dire le résultat positif) au destinataire. Les informations nécessaires pour prouver la source et l'intégrité des données sont consignées par une tierce partie. Dans ce cas, E ne peut pas nier par la suite avoir envoyé l'unité de données signée.

FIGURE A-2/X.800

Schéma de signature arbitré

A.4.4 *Mécanismes de contrôle d'accès*

Les mécanismes de contrôle d'accès sont ceux qui sont utilisés pour appliquer une politique de limitation de l'accès à une ressource aux seuls utilisateurs autorisés. Ces techniques comprennent l'utilisation de listes ou de matrices de contrôle d'accès (qui contiennent généralement les identités des articles contrôlés et des utilisateurs autorisés; ces utilisateurs sont, par exemple, des personnes ou des processus); ces techniques utilisent aussi des mots de passe et des capacités, étiquettes ou jetons dont la possession peut être utilisée pour indiquer des droits d'accès. Lorsque des capacités sont utilisées, elles devraient être non falsifiables et être acheminées de façon sûre.

A.4.5 *Mécanismes d'intégrité des données*

Les mécanismes d'intégrité des données sont de deux types: ceux qui sont utilisés pour protéger l'intégrité d'une seule unité de données et ceux qui protègent à la fois l'intégrité d'une seule unité de données et la séquence des unités de données au cours d'une connexion.

A.4.5.1 *Détection de modifications du train de messages*

Les techniques de détection de modifications, normalement associées à la détection d'erreurs de bits, d'erreurs de bloc et d'erreurs de mise en séquence, introduites par les liaisons et réseaux de communication peuvent également être utilisées pour détecter des modifications du train de messages. Cependant, si les en-têtes et les données de fin de protocole ne sont pas protégés par des mécanismes d'intégrité, tout intrus informé peut réussir à court-circuiter ces vérifications. On ne peut donc réussir à détecter une modification du train de messages qu'en utilisant des techniques de détection de modifications en relation avec des informations relatives à la séquence des données. Cela n'empêchera pas la modification du flux de messages, mais permettra de signaler les attaques.

A.4.6 *Mécanismes d'échange d'authentification*

A.4.6.1 *Choix des mécanismes*

Les choix et les combinaisons de mécanismes d'échange d'authentification appropriés à différentes circonstances sont nombreux. Par exemple:

a) lorsque des entités homologues et les moyens de communication sont fiables, l'identification d'une entité homologue peut être confirmée par un mot de passe. Le mot de passe protège des erreurs, mais il n'est pas une garantie contre la malveillance (en particulier, pas contre le fait de répéter). L'authentification mutuelle peut se faire en utilisant un mot de passe différent dans chaque direction;

b) lorsque chaque entité a confiance en ses entités homologues, mais ne peut pas se fier aux moyens de communication, la protection contre des attaques actives peut être fournie par des combinaisons de mots de passe et de chiffrement ou par des moyens cryptographiques. La protection contre le fait de répéter nécessite deux échanges (avec des paramètres de protection) ou une indication horaire (avec des horloges fiables). L'authentification mutuelle avec protection contre le fait de répéter peut être réalisée en trois échanges;

c) lorsque des entités n'ont pas confiance (ou pensent que, à l'avenir, elles ne pourraient pas avoir confiance) en leurs entités homologues ou des moyens de communication, des services de non-répudiation peuvent être utilisés. Le service de non-répudiation peut être fourni à l'aide des mécanismes de signature numérique et/ou de notarisation. Ces mécanismes peuvent être utilisés avec ceux qui sont décrits en b).

A.4.7 *Mécanismes de bourrage*

La production de trafic parasite et le bourrage d'unités de protocole jusqu'à une longueur fixe peuvent fournir une protection limitée contre l'analyse de trafic. Pour réussir, le niveau de trafic parasite doit s'approcher le plus possible du niveau prévu le plus élevé de trafic réel. En outre, le contenu des unités de données de protocole doit être chiffré ou déguisé de telle sorte que le trafic parasite ne puisse pas être identifié et différencié du trafic réel.

A.4.8 *Mécanisme de contrôle de routage*

La spécification des interdits de routage pour le transfert de données (y compris la spécification d'une route entière) peut être utilisée pour s'assurer que les données ne sont acheminées que par des routes physiquement sûres ou pour s'assurer que les informations sensibles ne sont acheminées que par des routes ayant un niveau de protection approprié.

A.4.9 *Mécanisme de notarisation*

Le mécanisme de notarisation est fondé sur le concept d'une tierce partie de confiance (un notaire) pour garantir certaines propriétés relatives aux informations échangées entre deux entités, telles que leur origine, leur intégrité ou l'heure à laquelle elles ont été envoyées ou reçues.

A.4.10 *Sécurité physique et personnel sûr*

Les mesures de sécurité physique seront toujours nécessaires pour garantir une protection complète. La sécurité physique est coûteuse, et l'on essaie souvent de réduire au minimum les besoins en sécurité physique en utilisant d'autres techniques (meilleur marché). Les considérations en matière de sécurité physique et de personnel n'entrent pas dans le cadre de l'OSI, bien que tous les systèmes reposent en fin de compte sur une certaine forme de sécurité physique et sur la confiance faite au personnel qui fait fonctionner le système. Des procédures de fonctionnement devraient être définies pour garantir un fonctionnement correct et pour délimiter les responsabilités du personnel.

A.4.11 *Matériel/logiciel de confiance*

Les méthodes utilisées pour faire confiance au fonctionnement correct d'une entité comprennent des méthodes de preuves formelles, la vérification et la validation, la détection et l'enregistrement de tentatives d'attaque, et la construction de l'entité par un personnel de confiance dans un environnement sûr. Il faut également veiller à ce que l'entité ne soit pas accidentellement ou délibérément modifiée de façon à compromettre la sécurité pendant sa durée de vie; par exemple, pendant la maintenance ou des opérations d'extension. Si l'on doit maintenir la sécurité, il faut se fier au fonctionnement correct de certaines entités. Les méthodes utilisées pour établir la confiance n'entrent pas dans le cadre de l'OSI.

ANNEXE B

Justification du placement des services et mécanismes de sécurité spécifiés au § 7

(La présente annexe ne fait pas partie intégrante de la Recommandation)

B.1 *Considérations générales*

La présente annexe donne quelques-unes des raisons pour lesquelles les services de sécurité ont été placés dans les différentes couches, comme indiqué au § 7. Les principes de la répartition en couches de la sécurité, identifiés au § 6.1.1 de la présente Recommandation, ont guidé cette répartition.

Un service de sécurité particulier est fourni par plus d'une couche si l'effet sur la sécurité générale de la communication est différent (par exemple, confidentialité de la connexion dans les couches 1 et 4). Néanmoins, si l'on considère les fonctionnalités existantes de la communication de données OSI (par exemple, les procédures multiliaisons, la fonction de multiplexage, les différentes façons d'améliorer un service en mode sans connexion en un service en mode connexion) et afin de permettre à ces mécanismes de transmission de fonctionner, il peut être nécessaire de permettre la fourniture d'un service particulier au niveau d'une autre couche, bien que l'on ne puisse pas considérer que l'effet sur la sécurité soit différent.

B.2 *Authentification de l'entité homologue*

- *Couches 1 et 2:* Non, l'authentification de l'entité homologue n'est pas jugée utile dans ces couches.
- *Couche 3:* Oui, pour des sous-réseaux individuels, pour le routage et/ou via l'interréseau.
- *Couche 4:* Oui, l'authentification de système d'extrémité à système d'extrémité dans la couche 4 peut servir à authentifier mutuellement deux entités de session ou plus, avant le début d'une connexion et pour la durée de cette connexion.
- *Couche 5:* Non, on n'a aucun intérêt à fournir ce service au niveau de la couche 4 et/ou des couches supérieures.

– *Couche 6:* Non, mais des mécanismes de chiffrement peuvent prendre en charge ce service dans la couche application.

– *Couche 7:* Oui, l'authentification de l'entité homologue devrait être fournie par la couche application.

B.3 *Authentification de l'origine des données*

– *Couches 1 et 2:* Non, l'authentification de l'origine des données n'est pas jugée utile dans ces couches.

– *Couches 3 et 4:* L'authentification de l'origine des données peut être fournie de bout en bout par la fonction de relais et de routage de la couche 3 et/ou dans la couche 4 comme suit:

  a) la fourniture de l'authentification de l'entité homologue au moment de l'établissement de la connexion avec authentification continue fondée sur le chiffrement, pendant la durée de vie d'une connexion, fournit *de facto* le service d'authentification de l'origine des données;

  b) même lorsque a) n'est pas fournie, l'authentification de l'origine des données fondée sur le chiffrement peut être fournie, avec très peu de frais supplémentaires, en plus de ceux liés aux mécanismes d'intégrité des données déjà placés dans ces couches.

– *Couche 5:* Non, on n'a aucun intérêt à fournir ce service au niveau de la couche 4 ou de la couche 7.

– *Couche 6:* Non, mais des mécanismes de chiffrement peuvent prendre en charge ce service dans la couche d'application.

– *Couche 7:* Oui, éventuellement en relation avec des mécanismes de la couche présentation.

B.4 *Contrôle d'accès*

– *Couches 1 et 2:* Les mécanismes de contrôle d'accès ne peuvent pas être fournis dans les couches 1 ou 2, dans un système conforme aux protocoles OSI, étant donné qu'il n'y a pas de facilité d'extrémité disponible pour ce type de mécanisme.

– *Couche 3:* Les mécanismes de contrôle d'accès peuvent être imposés à la fonction d'accès au sous-réseau par les exigences d'un sous-réseau particulier. Lorsqu'ils sont mis en œuvre par la fonction de relais et de routage, les mécanismes d'accès de la couche réseau peuvent être utilisés à la fois pour contrôler l'accès aux sous-réseaux par les entités relais et pour contrôler l'accès aux systèmes d'extrémité. En clair, le niveau d'accès est relativement grossier, la distinction ne se faisant qu'entre les entités de la couche réseau.

  L'établissement d'une connexion de réseau peut souvent se traduire par une facturation établie par l'administration du sous-réseau. Le contrôle d'accès et l'acceptation de taxation à l'arrivée ou le choix d'autres paramètres de réseau ou sous-réseau peuvent minimiser les coûts.

– *Couche 4:* Oui, les mécanismes de contrôle d'accès peuvent être utilisés, connexion de transport de bout en bout par connexion.

– *Couche 5:* Non, on n'a aucun intérêt à fournir ce service dans la couche 4 et/ou dans la couche 7.

– *Couche 6:* Non, ce mécanisme n'est pas approprié pour la couche 6.

– *Couche 7:* Oui, les protocoles d'application et/ou les processus d'application peuvent fournir des facilités supplémentaires de contrôle d'accès, axées sur l'application.

B.5 *Confidentialité de toutes les données utilisateur en mode connexion*

– *Couche 1:* Oui, devrait être fournie étant donné que l'insertion électrique de paires transparentes de dispositifs de transformation peut assurer une confidentialité complète sur une connexion physique.

– *Couche 2:* Oui, mais cela ne donne pas une meilleure sécurité pour la couche 1 ou pour la couche 3.

– *Couche 3:* Oui, pour une fonction d'accès au sous-réseau sur des sous-réseaux individuels et les fonctions de relais et de routage sur l'interréseau.

– *Couche 4:* Oui, étant donné que la connexion de transport assure un mécanisme de transport de bout en bout et peut fournir l'isolation des connexions de session.

– *Couche 5:* Non, étant donné que cela n'améliore pas la confidentialité dans les couches 3, 4 et 7. Il ne semble pas approprié de fournir ce service dans cette couche.

– *Couche 6:* Oui, étant donné que des mécanismes de chiffrement ne fournissent que des transformations purement syntaxiques.

– *Couche 7:* Oui, en relation avec des mécanismes des couches inférieures.

B.6 *Confidentialité de toutes les données utilisateur d'une SDU en mode sans connexion*

La justification est la même que pour la confidentialité de toutes les données utilisateur en mode connexion, sauf pour la couche 1 où il n'y a pas de service sans connexion.

B.7 *Confidentialité sélective par champ dans les données utilisateur d'une SDU*

Ce service de confidentialité est fourni par le mécanisme chiffrement dans la couche présentation et il est pris en charge par des mécanismes de la couche application suivant la sémantique des données.

B.8 *Confidentialité du flux de données*

La confidentialité totale du flux de données ne peut être réalisée que dans la couche 1 par l'insertion physique d'une paire de dispositifs de chiffrement dans la voie de transmission physique. On suppose que la voie de transmission sera bidirectionnelle simultanée et synchrone, de sorte que l'insertion des dispositifs rendra toutes les transmissions (même leur présence) sur les supports physiques non reconnaissables.

Au-dessus de la couche physique, il est impossible d'avoir une sécurité totale du flux de données dont certains des effets peuvent être en partie obtenus par l'utilisation d'un service complet de confidentialité des SDU dans une couche et par l'injection de flux parasites dans une couche supérieure. Ce type de mécanisme est coûteux et c'est un consommateur potentiel de grandes quantités de capacités de transit et de commutation.

Si la confidentialité du flux de données est fournie dans la couche 3, le bourrage et/ou le contrôle de routage seront utilisés. Le contrôle de routage peut fournir une confidentialité limitée du flux de données en acheminant les messages hors des liaisons ou des sous-réseaux peu sûrs. Cependant, l'incorporation d'un bourrage dans la couche 3 permet de mieux utiliser le réseau, par exemple en évitant un bourrage inutile et un encombrement du réseau.

Une confidentialité limitée du flux de données peut être fournie dans la couche application par la production de parasites en relation avec la confidentialité servant à empêcher l'identification des parasites.

B.9 *Intégrité de toutes les données utilisateur en mode connexion (avec reprise sur erreur)*

– *Couches 1 et 2:* Les couches 1 et 2 ne peuvent pas fournir ce service. La couche 1 n'a aucun mécanisme de détection ou de reprise, et le mécanisme de la couche 2 ne fonctionne que point à point et non de bout en bout; par conséquent, la fourniture de ce service n'est pas jugée utile.

– *Couche 3:* Non, étant donné que la reprise sur erreur n'est pas disponible universellement.

– *Couche 4:* Oui, étant donné que ce service fournit la connexion de transport de bout en bout.

– *Couche 5:* Non, étant donné que la reprise sur erreur n'est pas une fonction de la couche 5.

– *Couche 6:* Non, mais les mécanismes de chiffrement peuvent prendre en charge ce service dans la couche application.

– *Couche 7:* Oui, en relation avec des mécanismes de la couche présentation.

B.10 *Intégrité de toutes les données utilisateur en mode connexion (sans reprise sur erreur)*

– *Couches 1 et 2:* Les couches 1 et 2 ne peuvent pas fournir ce service. La couche 1 n'a aucun mécanisme de détection ou de reprise, et le mécanisme de la couche 2 ne fonctionne que point à point et non de bout en bout. Par conséquent, la fourniture de ce service n'est pas jugée utile.

– *Couche 3:* Oui, pour la fonction d'accès au sous-réseau sur les sous-réseaux individuels et pour les fonctions de routage et de relais sur l'interréseau.

– *Couche 4:* Oui, pour les cas où il est acceptable d'arrêter la communication après détection d'une attaque active.

– *Couche 5:* Non, étant donné que ce service n'apporte rien de plus par rapport à l'intégrité des données fournie dans les couches 3, 4 ou 7.

– *Couche 6:* Non, mais des mécanismes de chiffrement peuvent prendre en charge ce service dans la couche application.

– *Couche 7:* Oui, en relation avec des mécanismes de la couche présentation.

B.11 *Intégrité sélective par champ des données utilisateur de SDU en mode connexion (sans reprise)*

L'intégrité sélective par champ peut être fournie par des mécanismes de chiffrement dans la couche présentation avec des mécanismes d'appel et de vérification dans la couche application.

B.12 *Intégrité de toutes les données utilisateur d'une SDU en mode sans connexion*

Afin de réduire au minimum la duplication des fonctions, l'intégrité des transferts en mode sans connexion ne devrait être fournie que dans les mêmes couches que l'intégrité sans reprise, c'est-à-dire dans la couche réseau, la couche transport et la couche application. Ces mécanismes d'intégrité ne peuvent avoir qu'une efficacité très limitée.

B.13 *Intégrité sélective par champ dans une SDU en mode sans connexion*

L'intégrité sélective par champ peut être fournie par des mécanismes de chiffrement dans la couche présentation conjointement avec des mécanismes d'appel et de contrôle dans la couche application.

B.14 *Non-répudiation*

Les services de non-répudiation avec preuve de l'origine et de la remise peuvent être fournis par un mécanisme de notarisation qui comprendra un relais dans la couche 7.

L'utilisation du mécanisme de signature numérique pour la nonrépudiation nécessite une coopération étroite entre les couches 6 et 7.

ANNEXE C

Choix du placement du mécanisme de chiffrement pour les applications

(La présente annexe ne fait pas partie intégrante de la Recommandation)

C.1 La plupart des applications ne nécessiteront pas de chiffrement dans plus d'une couche. Le choix de la couche dépend de certains éléments importants qui sont décrits ci-dessous:

1) si une confidentialité totale du flux de données est exigée, le chiffrement dans la couche physique ou la sécurité de transmission (par exemple, des techniques appropriées de sécurité à spectre étalé), seront choisis. Une sécurité physique adéquate, un routage fiable, ainsi qu'une fonctionnalité similaire au niveau des relais peuvent satisfaire à toutes les exigences de confidentialité;

2) si un niveau fin de protection (c'est-à-dire, une clé séparée pour chaque association d'application), la non-répudiation ou la protection sélective par champ sont exigés, le chiffrement dans la couche présentation sera choisi. La protection sélective par champ peut être importante car les algorithmes de chiffrement consomment de grandes quantités de puissance de traitement. Le chiffrement dans la couche présentation peut fournir l'intégrité sans reprise, la non-répudiation et la confidentialité totale;

3) si une protection globale simple de toutes les communications de système d'extrémité à système d'extrémité et/ou un dispositif de chiffrement externe sont souhaités (par exemple, pour assurer une protection physique à l'algorithme et aux clés ou une protection contre un logiciel défectueux), le chiffrement dans la couche réseau sera choisi. Cela peut fournir la confidentialité et l'intégrité sans reprise.

   Remarque – Bien que la reprise ne soit pas fournie dans la couche réseau, les mécanismes normaux de reprise dans la couche transport peuvent être utilisés pour déclencher une reprise sur des attaques détectées par la couche réseau;

4) si l'intégrité avec reprise, avec une protection très détaillée, est exigée, le chiffrement de la couche transport sera choisi. Cela peut fournir la confidentialité et l'intégrité avec ou sans reprise;

5) le chiffrement au niveau dans la couche liaison de données n'est pas recommandé pour les futures réalisations.

C.2 Lorsque plusieurs de ces critères sont retenus, le chiffrement peut devoir être fourni dans plus d'une couche.