NORME INTERNATIONALE

ISO 7498-2

Première édition
1989-02-15

Systèmes de traitement de l'information — Interconnexion de systèmes ouverts — Modèle de référence de base

Partie 2 : Architecture de sécurité

Information processing systems — Open Systems Interconnection — Basic Reference Model Part 2 : Security Architecture

Numéro référence
ISO 7498-2 : 1989 (F)

Avant-propos

L'ISO (Organisation internationale de normalisation) est une fédération mondiale d'organismes nationaux de normalisation (comités membres de l'ISO). L'élaboration des Normes internationales est en général confiée aux comités techniques de l'ISO. Chaque comité membre intéressé par une étude a le droit de faire partie du comité technique créé à cet effet. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO participent également aux travaux. L'ISO collabore étroitement avec la Commission électrotechnique internationale (CEI) en ce qui concerne la normalisation électrotechnique.

Les projets de Normes internationales adoptés par les comités techniques sont soumis aux comités membres pour approbation, avant leur acceptation comme Normes internationales par le Conseil de l'ISO. Les Normes internationales sont approuvées conformément aux procédures de l'ISO qui requièrent l'approbation de 75 % au moins des comités membres votants.

La Norme internationale ISO 7498-2 a été élaborée par le comité technique ISO/TC 97, *Systèmes de traitement de l'information*.

L'attention des utilisateurs est attirée sur le fait que toutes les Normes internationales sont de temps en temps soumises à révision et que toute référence faite à une autre norme internationale dans le présent document implique qu'il s'agit, sauf indication contraire, de la dernière édition.

Organisation internationale de normalisation
Case postale 56 • CH-1211 Genève 20 • Suisse
Version française tirée en 1990

Imprimé en Suisse

Sommaire

Page blanche

Systèmes de traitement de l'information — Interconnexion de systèmes ouverts — Modèle de référence de base —

Partie 2 : Architecture de sécurité

0 Introduction

L'ISO 7498 décrit le Modèle de référence de base pour l'interconnexion de systèmes ouverts (OSI). L'ISO 7498 établit un cadre permettant de coordonner le développement des normes existantes et à venir pour l'interconnexion des systèmes.

L'objectif de l'OSI est de permettre l'interconnexion de systèmes hétérogènes d'ordinateurs 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 des données plus important que la valeur potentielle de cette action ou allonger tellement la durée requise pour obtenir les données que la valeur des données serait perdue.

La présente partie de l'ISO 7498 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 normes existantes ou d'élaborer de nouvelles normes 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 Norme internationale. Il est conseillé au lecteur n'ayant pas ces connaissances de lire en premier l'annexe A.

La présente partie de l'ISO 7498 est une extension du Modèle de référence de base 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 de base.

1 Objet et domaine d'application

La présente partie de l'ISO 7498 :

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

b) définit où, dans l'architecture OSI, les services et mécanismes peuvent être fournis.

La présente partie de l'ISO 7498 élargit le champ d'application de l'ISO 7498 afin de couvrir les communications sûres entre systèmes ouverts.

Des services et des mécanismes de sécurité de base et leur placement approprié ont été identifiés pour toutes les couches du Modèle de référence de base. En outre, les relations architecturales entre les services et mécanismes de sécurité et le Modèle de référence de base ont été identifiées. Des mesures supplémentaires de sécurité peuvent être nécessaires dans des systèmes 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 est en dehors du champ d'application de la présente Norme internationale.

Les fonctions de sécurité OSI ne concernent que les aspects visibles d'une voie de communication permettant aux systèmes extrémité de réaliser entre eux un transfert sûr d'informations. La sécurité OSI ne concerne pas des mesures de sécurité nécessaires dans les systèmes 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 normes OSI.

La présente partie de l'ISO 7498 complète les concepts et principes définis dans l'ISO 7498 ; elle ne les modifie pas. Elle ne constitue ni une spécification de réalisation de systèmes, ni une base d'évaluation de la conformité de réalisations de systèmes.

2 Références

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 général de gestion.*

ISO 7498/Add.1, *Systèmes de traitement de l'information — Interconnexion de systèmes ouverts — Modèle de référence de base. — Additif 1 : Transmission en mode sans connexion.*

ISO 8648, *Systèmes de traitement de l'information — Interconnexion de systèmes ouverts — Organisation interne de la Couche Réseau.*

3 Définitions et abréviations

3.1 La présente partie de l'ISO 7498 se fonde sur les concepts élaborés dans l'ISO 7498 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 ; et
t) syntaxe de transfert.

3.2 La présente partie de l'ISO 7498 utilise les termes suivants définis dans les Normes internationales citées en référence.

Transmission en mode sans connexion	(ISO 7498/Add.1)
Système extrémité	(ISO 7498)
Fonction de relais et de routage	(ISO 8648)
UNITDATA	(ISO 7498)
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 ; et (Security Management Information Base)
MIB base d'informations de gestion. (Management Information Base)

3.3 Pour les besoins de la présente partie de l'ISO 7498,les définitions suivantes sont applicables :

3.3.1 contrôle d'accès : Précaution prise contre l'utilisation non autorisée d'une ressource ; ceci 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 autorisées à accéder à une ressource ; cette liste inclut les droits d'accès liés aux entités.

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.

NOTE — La modification et le fait de rejouer des 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 «**journal d'audit de sécurité**» (3.3.48).

3.3.7 authentification : voir «**authentification de l'origine l'origine des données**» et «**authentification de l'entité homologue**» (3.3.22 et 3.3.40).

NOTE — Dans la présente partie de l'ISO 7498, 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 les 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.

NOTE — Le **cryptogramme** peut lui-même être réinjecté dans un nouveau chiffrement pour produire un **cryptogramme** sur-chiffré.

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 (voir **cryptographie**) sur une unité de données.

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

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.

NOTE — La cryptographie détermine les méthodes de chiffrement et de déchiffrement. Une attaque portant sur les principes, moyens et méthodes de cryptographie est appelée une 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 déchiffrement : Opération inverse d'un chiffrement réversible.

3.3.24 décryptage : voir **déchiffrement**.

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 (voir **cryptographie**) 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 chiffrement : Transformation cryptographique (voir **cryptographie**) de données produisant un **cryptogramme**.

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

3.3.28 cryptage : voir **chiffrement**.

3.3.29 chiffrement de bout en bout : **Chiffrement** de données à l'intérieur ou au niveau du système extrémité source, le **déchiffrement** correspondant ne se produisant qu'à l'intérieur, ou au niveau du système extrémité de destination. [Voir aussi **chiffrement de liaison (liaison par liaison)** (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 du système. [Voir aussi «**chiffrement de bout en bout**», (3.3.29)].

NOTE — 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 déguisement : 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.

NOTE — Ce terme étant lié au droit privé, il ne peut pas être très précis et son utilisation devrait être évitée sauf pour des besoins de sécurité.

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 de l'activité 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 politiques 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).

NOTE — 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)].

NOTE — Une politique de sécurité complète traite nécessairement de sujets qui sont hors 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 définis par une politique de sécurité, par exemple.

4 Notation

La notation utlisée pour désigner les couches est la même que celle définie dans l'ISO 7498.

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 œuvre ces services sont présentés dans le présent article. 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 (preuves 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 plusieurs entités connectées à une ou plusieurs autres entités. Ce service garantit — uniquement lors de son utilisation — qu'une entité n'essaie pas de se déguiser ou de rejouer 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 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 de l'utilisateur (N) au cours d'une connexion (N).

NOTE — 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 de l'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 de l'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.

NOTE — 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 de l'utilisateur (N) au cours d'une connexion (N) et détecte toute donnée modifiée, insérée, supprimée ou rejouée 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 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 de l'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 rejoués.

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) en demande.

Ce service assure l'intégrité d'une unité unique 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 rejouée 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 protègera 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 en 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 et ;

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 paragraphe 8.4 donne certaines 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 ; et
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. Donc, 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

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 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 de 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 ;

NOTE — 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, généralement conformément à une politique de sécurité ;

e) heure de la tentative d'accès ;

f) route de la tentative d'accès ; et

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 connues à priori du côté de l'entité source. Ces besoins doivent être enregistrés dans la base d'informations de gestion de sécurité (voir 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 flot d'unités de données ou d'un flot de champs d'unité 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 destinataire. L'entité émettrice ajoute à une unité de données une quantité qui est une fonction de la donnée. Cette quantité 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 destinataire génère une quantité correspondante et la compare à la quantité

reçue pour déterminer si les données ont été modifiées pendant le transit. Ce mécanisme seul ne protègera pas contre le fait de rejouer une unité de données unique. Dans des 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, le fait de rejouer, 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 rejouer 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 :

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

b) techniques cryptographiques ; et

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 rejouer (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 unilarérale et mutuelle) ; et

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

5.3.6 Mécanismes 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 extémité 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

Des propriétés relatives à des données communiquées entre deux ou plusieurs entités, 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, à l'article 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 l'article 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 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 norme 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 Étiquettes de sécurité

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 logon). 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 de traitement d'événements (voir 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 5.4.3) ; et

d) action de reprise (voir 5.4.4).

Des exemples d'événements liés à la sécurité sont :

a) une violation spécifique de la sécurité ;

b) un événement spécifique choisi ; et

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

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

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 de la production de rapports sont considérées comme une fonction de gestion de sécurité (voir 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 ; et

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 candidats à la normalisation comprennent des protocoles pour les actions de reprise et pour la gestion de reprise de sécurité (voir 8.3.3).

5.5 Illustration de la relation entre services et mécanismes de sécurité

Le tableau 1 **montre** quels mécanismes, seuls ou combinés à d'autres, sont considérés comme étant parfois appropriés pour fournir 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 en 5.2 et en 5.3. Les relations sont décrites plus complètement à l'article 6.

6 Relations 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 pour 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 ;