UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T X.803

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

(07/94)

RÉSEAUX DE COMMUNICATION DE DONNÉES ET COMMUNICATION ENTRE SYSTÈMES OUVERTS

SÉCURITÉ

TECHNOLOGIES DE L'INFORMATION – INTERCONNEXION DES SYSTÈMES OUVERTS – MODÈLE DE SÉCURITÉ POUR LES COUCHES SUPÉRIEURES

Recommandation UIT-T X.803

(Antérieurement «Recommandation du CCITT»)

AVANT-PROPOS

L'UIT (Union internationale des télécommunications) est une institution spécialisée des Nations Unies dans le domaine des télécommunications. L'UIT-T (Secteur de la normalisation des télécommunications) est un organe permanent de l'UIT. Au sein de l'UIT-T, qui est l'entité qui établit les normes mondiales (Recommandations) sur les télécommunications, participent quelque 179 pays membres, 84 exploitations de télécommunications reconnues, 145 organisations scientifiques et industrielles et 38 organisations internationales.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution nº 1 de la Conférence mondiale de normalisation des télécommunications (CMNT), (Helsinki, 1993). De plus, la CMNT, qui se réunit tous les quatre ans, approuve les Recommandations qui lui sont soumises et établit le programme d'études pour la période suivante.

Dans certains secteurs de la technologie de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI. Le texte de la Recommandation X.803 de l'UIT-T a été approuvé le 1er juillet 1994. Son texte est publié, sous forme identique, comme Norme internationale ISO/CEI 10745.

NOTE

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

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE COMMUNICATION DE DONNÉES ET COMMUNICATION ENTRE SYSTÈMES OUVERTS

(Février 1994)

ORGANISATION DES RECOMMANDATIONS DE LA SÉRIE X

Domaine	Recommandations
RÉSEAUX PUBLICS POUR DONNÉES	
Services et services complémentaires	X.1-X.19
Interfaces	X.20-X.49
Transmission, signalisation et commutation	X.50-X.89
Aspects réseau	X.90-X.149
Maintenance	X.150-X.179
Dispositions administratives	X.180-X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	
Modèle et notation	X.200-X.209
Définition des services	X.210-X.219
Spécifications des protocoles en mode connexion	X.220-X.229
Spécifications des protocoles en mode sans connexion	X.230-X.239
Formulaires PICS	X.240-X.259
Identification des protocoles	X.260-X.269
Protocoles de sécurité	X.270-X.279
Objets gérés de couche	X.280-X.289
Test de conformité	X.290-X.299
INTERFONCTIONNEMENT DES RÉSEAUX	
Considérations générales	X.300-X.349
Systèmes mobiles de transmission de données	X.350-X.369
Gestion	X.370-X.399
SYSTÈMES DE MESSAGERIE	X.400-X.499
ANNUAIRE	X.500-X.599
RÉSEAUTAGE OSI ET ASPECTS DES SYSTÈMES	
Réseautage	X.600-X.649
Dénomination, adressage et enregistrement	X.650-X.679
Notation de syntaxe abstraite numéro un (ASN.1)	X.680-X.699
GESTION OSI	X.700-X.799
SÉCURITÉ	X.800-X.849
APPLICATIONS OSI	
Engagement, concomitance et rétablissement	X.850-X.859
Traitement des transactions	X.860-X.879
Opérations distantes	X.880-X.899
TRAITEMENT OUVERT RÉPARTI	X.900-X.999

TABLE DES MATIÈRES

Introduction et Résumé

L'architecture de sécurité OSI (Rec. X.800 du CCITT | ISO 7498-2) définit les éléments d'architecture relatifs à la sécurité convenant à une application lorsqu'il faut assurer une protection de sécurité dans un environnement de systèmes ouverts.

La présente Recommandation | Norme internationale décrit la sélection, l'insertion et l'utilisation des services et mécanismes de sécurité dans les couches supérieures (application, présentation et session) du Modèle de référence OSI.

NORME INTERNATIONALE

RECOMMANDATION UIT-T

TECHNOLOGIES DE L'INFORMATION – INTERCONNEXION DES SYSTÈMES OUVERTS – MODÈLE DE SÉCURITÉ POUR LES COUCHES SUPÉRIEURES

1 Domaine d'application

1.1 La présente Recommandation | Norme internationale définit un modèle d'architecture sur lequel est fondé:

a) le développement de services et de protocoles indépendants des applications, pour la sécurité dans les couches supérieures OSI; et

b) l'utilisation de ces services et protocoles de manière à satisfaire aux conditions de sécurité d'une large gamme d'applications afin que les éléments ASE spécifiques à l'application contiennent le minimum de services de sécurité.

1.2 La présente Recommandation | Norme internationale spécifie en particulier:

a) les aspects de sécurité de la communication dans les couches supérieures OSI;

b) la prise en charge, dans les couches supérieures, des services de sécurité définis dans l'architecture de sécurité OSI et dans les Cadres de sécurité pour les systèmes ouverts;

c) l'insertion des services et mécanismes de sécurité et leurs relations dans les couches supérieures, conformément à la Rec. X.800 du CCITT | ISO 7498-2 et à la Rec. UIT-T X.207 | ISO/CEI 9545;

d) les interactions entre couches supérieures ainsi que les interactions entre couches supérieures et couches inférieures lors de la fourniture et de l'utilisation des services de sécurité;

e) les conditions de gestion des informations de sécurité dans les couches supérieures.

1.3 En ce qui concerne le contrôle d'accès, le domaine d'application de la présente Recommandation | Norme internationale comprend les services et mécanismes permettant de contrôler l'accès aux ressources OSI et aux ressources accessibles par l'intermédiaire de l'OSI.

1.4 La présente Recommandation | Norme internationale ne couvre pas:

a) la définition de services OSI ni la spécification de protocoles OSI;

b) la spécification de techniques et de mécanismes de sécurité, leur fonctionnement ou leur utilisation dans des protocoles;

c) les aspects de la sécurité non relatifs aux communications OSI.

1.5 La présente Recommandation | Norme internationale ne constitue ni une spécification de mise en œuvre de systèmes, ni une base d'évaluation de la conformité.

NOTE – Le domaine d'application de la présente Recommandation | Norme internationale s'étend à la sécurité des applications en mode sans connexion et à celle des applications réparties (applications en mode asynchrone, applications chaînées et applications agissant pour d'autres applications).

2 Références normatives

Les Recommandations et les Normes internationales suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions valables pour la présente Recommandation | Norme internationale. Au moment de la publication, les éditions indiquées étaient en vigueur. Toute Recommandation ou Norme internationale est sujette à révision et les parties prenantes aux accords fondés sur la présente Recommandation | Norme internationale sont

invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et Normes internationales indiquées ci-après. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur. Le Bureau de la normalisation des télécommunications de l'UIT-T tient à jour une liste des Recommandations UIT-T en vigueur.

2.1 Recommandations | Normes internationales identiques

- Recommandation UIT-T X.207 (1993) | ISO/CEI 9545:1993, *Technologie de l'information – Interconnexion de systèmes ouverts – Structure de la couche application.*
- Recommandation UIT-T X.811[1)] | ISO/CEI 10181-2...[1)], *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour systèmes ouverts – Cadre d'authentification*.
- Recommandation UIT-T X.812[1)] | ISO/CEI 10181-3...[1)], *Technologie de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts – Cadre de contrôle d'accès*.

2.2 Paires de Recommandations | Normes internationales équivalentes par leur contenu technique

- Recommandation X.200 du CCITT (1988), *Modèle de référence pour l'interconnexion des systèmes ouverts pour les applications du CCITT.*

  ISO 7498:1984/Cor.1:1988, *Systèmes de traitement de l'information – Interconnexion des systèmes ouverts – Modèle de référence de base*.
- Recommandation X.216 du CCITT (1988), *Définition du service de présentation de l'OSI (Interconnexion des systèmes ouverts) pour les applications du CCITT*.

  ISO 8822:1987, *Systèmes de traitement de l'information – Interconnexion des systèmes ouverts – Définition du service de présentation en mode connexion*.
- Recommandation X.217 du CCITT (1988), *Définition du service de contrôle d'association pour l'interconnexion des systèmes ouverts pour les applications du CCITT*.

  ISO 8649:1987, *Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Définition du service pour l'élément de service de contrôle d'association*.
- Recommandation X.700 du CCITT (1992), *Cadre de gestion pour l'interconnexion des systèmes ouverts pour les applications du CCITT*.

  ISO/CEI 7498-4:1989, *Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Modèle de référence de base. Partie 4: Cadre général de gestion*.
- Recommandation X.800 du CCITT (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT*.

  ISO 7498-2:1988, *Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Modèle de référence de base – Partie 2: Architecture de sécurité*.

3 Définitions

3.1 Les termes suivants, définis dans la Rec. X.200 du CCITT | ISO 7498, sont utilisés:

a) syntaxe abstraite;

b) entité d'application;

c) processus d'application;

d) invocation de processus d'application;

e) informations de contrôle de protocole d'application;

f) unité de données de protocole d'application;

g) environnement de système local;

h) fonction (N);

---

1) Actuellement à l'état de projet.

i) relais (N);
j) système ouvert;
k) contexte de présentation;
l) entité de présentation;
m) système ouvert réel;
n) gestion-système;
o) syntaxe de transfert.

3.2 Les termes suivants définis dans la Rec. X.800 du CCITT | ISO 7498-2 sont utilisés:

a) contrôle d'accès;
b) authentification;
c) confidentialité;
d) intégrité des données;
e) authentification de l'origine des données;
f) déchiffrement;
g) chiffrement;
h) clé;
i) non-répudiation;
j) notarisation;
k) authentification de l'entité homologue;
l) vérification de sécurité;
m) base d'informations sur la gestion de la sécurité;
n) politique de sécurité;
o) protection sélective des champs;
p) signature;
q) confidentialité des flux de trafic;
r) fonctionnalité de confiance.

3.3 Les termes suivants définis dans la Rec. X.700 du CCITT | ISO/CEI 7498-4 sont utilisés:

a) informations de gestion;
b) gestion OSI.

3.4 Les termes suivants définis dans la Rec. UIT-T X.207 | ISO/CEI 9545 sont utilisés:

a) association d'applications;
b) contexte d'application;
c) invocation d'entité d'application (AEI);
d) élément de service d'application (ASE);
e) type d'élément ASE;
f) objet de service d'application (ASO);
g) association d'objets ASO;
h) contexte d'objet ASO;
i) invocation d'objet ASO;
j) type d'objet ASO;
k) fonction de contrôle (CF).

3.5 Le terme suivant défini dans la Rec. X.216 du CCITT | ISO 8822 est utilisé:

– valeur de données de présentation.

3.6 Les termes suivants définis dans la Rec. UIT-T X.811 | ISO/CEI 10181-2 sont utilisés:

a) échange pour authentification;

b) informations d'authentification pour déclaration;

c) déclarant;

d) informations d'authentification pour échange;

e) authentification d'entité;

f) entité principale,

g) information d'authentification pour vérification;

h) vérificateur.

3.7 Les termes suivants définis dans la Rec. UIT-T X.812 | ISO/CEI 10181-3 sont utilisés:

a) certificat de contrôle d'accès;

b) informations de contrôle d'accès.

3.8 Pour les besoins de la présente Recommandation | Norme internationale, les définitions suivantes s'appliquent:

état de sécurité par association: Etat de sécurité lié à une association de sécurité.

contexte de protection de la présentation: Contexte de présentation associant une syntaxe de protection du transfert à une syntaxe abstraite.

syntaxe de protection du transfert: Syntaxe de transfert fondée sur des processus de codage/décodage qui font appel à une transformation pour la sécurité.

sceau: Valeur de contrôle cryptographique supportant l'intégrité mais n'offrant pas de protection contre une falsification de la part du destinataire (c'est-à-dire, ne supportant pas la non-répudiation).

association de sécurité: Relation entre deux ou plus de deux entités pour lesquelles il existe des attributs (règles et informations d'état) régissant la fourniture des services de sécurité qui intéressent les entités en question.

fonction de communication de sécurité: Fonction supportant le transfert, entre systèmes ouverts, d'informations liées à la sécurité.

domaine de sécurité: Combinaison d'un ensemble d'éléments, d'une politique de sécurité, d'une autorité chargée de la sécurité et d'un ensemble d'activités relatives à la sécurité dont l'ensemble d'éléments est régi par la politique de sécurité, sous la responsabilité de l'autorité sur la sécurité, pour les activités spécifiées.

échange pour la sécurité: Transfert ou séquence de transferts d'informations de contrôle de protocole d'application entre systèmes ouverts, faisant partie intégrante d'un ou de plusieurs mécanismes de sécurité.

item d'échange pour la sécurité: Elément d'information distinct logiquement et correspondant à un transfert unique (d'une séquence de transferts) dans le cadre d'un échange pour la sécurité.

fonction d'échange pour la sécurité: Fonction de communication de sécurité, située dans la couche application, qui permet d'assurer la transmission d'informations relatives à la sécurité entre entités d'application invoquées.

règles d'interaction sécurisées: Aspects communs des règles qui régissent les interactions entre les domaines de sécurité.

état de sécurité: Informations d'état conservées dans un système ouvert et nécessaires à la fourniture des services de sécurité.

fonction de sécurité (de) système: Capacité d'un système ouvert à exécuter un traitement lié à la sécurité.

objet de sécurité (de) système: Objet représentant un ensemble de fonctions liées à la sécurité de système.

transformation pour la sécurité: Ensemble de fonctions (fonctions de sécurité de système et fonctions de communication de sécurité) qui agissent en combinaison sur les éléments de données d'usager pour en assurer la protection dans des conditions spécifiques pendant la communication ou le stockage.

NOTE – La spécification des fonctions et objets de sécurité-système ne fait pas partie intégrante des définitions de service de couche OSI ou des spécifications de protocole OSI.

4 Abréviations

Pour les besoins de la présente Recommandation | Norme internationale, les abréviations suivantes s'appliquent:

ACSE Elément de service de contrôle d'association (*association control service element*)

AE Entité d'application (*application-entity*)

AEI Invocation d'entité d'application (*application-entity-invocation*)

ASE Elément de service d'applications (*application-service-element*)

ASN.1 Notation de syntaxe abstraite numéro un (*abstract syntax notation one*)

ASO Objet de service d'application (*application-service-object*)

CF Fonction de contrôle (*control function*)

FTAM Transfert, accès et gestion de fichiers (*file transfer, access and management*)

OSI Interconnexion des systèmes ouverts (*open systems interconnection*)

PDV Valeur de données de présentation (*presentation data value*)

PE Entité de présentation (*presentation-entity*)

PEI Invocation d'entité de présentation (*presentation-entity-invocation*)

SEI Item d'échange pour la sécurité (*security exchange item*)

SSO Objet de sécurité de système (*system security object*)

5 Concepts

Le présent Modèle de sécurité décrit la fourniture des services de sécurité qui permettent de contrer les menaces relatives aux couches supérieures OSI, dont certains exemples sont présentés dans l'Annexe A de la Rec. X.800 du CCITT | ISO 7498-2. Ce modèle englobe la protection des informations qui passent par des systèmes de relais d'application.

5.1 Politique de sécurité

Pour que deux ou plus de deux systèmes ouverts réels puissent communiquer en toute sécurité, ils doivent être régis par les politiques de sécurité en vigueur dans leurs domaines de sécurité respectifs, ainsi que par une politique d'interaction sécurisée, si la communication est établie entre différents domaines de sécurité. Une politique d'interaction sécurisée couvre les aspects des politiques de sécurité qui sont communs à différentes domaines de sécurité et détermine les conditions dans lesquelles la communication peut être établie entre ces domaines.

Les dispositions d'une politique d'interaction sécurisée peuvent être décrites par un ensemble de règles qui régissent, entre autres, la sélection des contextes d'objet ASO (y compris celle des contextes d'application) à utiliser dans des cas précis de communication.

5.2 Associations de sécurité

Une association de sécurité est une relation entre deux ou plus de deux entités pour lesquelles il existe des attributs (règles et informations d'états) régissant la fourniture des services de sécurité qui intéressent les entités en question. Une association de sécurité implique l'existence d'une politique d'interaction sécurisée et le maintien d'un état de sécurité cohérent dans chacun des deux systèmes.

Du point de vue des couches supérieures OSI, une association de sécurité est appliquée sur une association d'objets ASO. En voici deux cas particuliers:

– *association de sécurité de type association d'applications* – Association de sécurité entre deux systèmes, supportant une communication en mode protégé par l'intermédiaire d'une association d'applications;

– *association de sécurité par relais* – Association de sécurité entre deux systèmes, supportant une communication en mode protégé par l'intermédiaire d'un relais d'application (par exemple, dans des applications en mode asynchrone ou chaînées);

Il existe d'autres exemples de types d'associations de sécurité, à savoir:

- association de sécurité entre deux systèmes qui communiquent directement entre eux par l'intermédiaire d'associations d'applications multiples et/ou par transmission de plusieurs unités de données en mode sans connexion;
- association de sécurité entre une entité inscrivant des informations en mode protégé dans une mémoire-données (par exemple mémoire-fichier ou répertoire) et des entités lisant ces informations;
- association de sécurité entre deux entités homologues de protocole de sécurité de couche inférieure.

Dans un processus d'application, une association de sécurité peut dépendre du maintien d'une autre association de sécurité avec un autre système, tel qu'un serveur d'authentification ou un autre type de tiers habilité.

5.3 Etat de sécurité

Un état de sécurité est une information d'état détenue dans un système ouvert réel et nécessaire à la fourniture de services de sécurité OSI. L'existence d'une association de sécurité entre processus d'application implique l'existence d'un état de sécurité partagée.

Il peut être nécessaire que certaines informations relatives à l'état de sécurité soient disponibles pour un ou plusieurs processus d'application avant les tentatives d'établissement des communications; elles peuvent être maintenues pendant les communications et/ou conservées après la fin des communications. La nature exacte des informations d'état dépend des mécanismes de sécurité et des applications.

On distingue deux catégories d'états de sécurité:

a) *état de sécurité de système* – Information d'état relative à la sécurité établie et maintenue dans un système ouvert réel, indépendamment de l'existence d'activités de communication ou de leur état;

b) *état de sécurité d'association* – Etat de sécurité relatif à une association de sécurité. Dans les couches supérieures OSI, l'état de sécurité partagée régit les (propriétés de sécurité des) contextes d'objet ASO utilisés entre les invocations d'objet ASD et/ou l'état initial de sécurité d'associations d'applications nouvellement établies, dont voici deux cas particuliers:

   - l'association de sécurité est appliquée sur une association d'applications unique. L'état de sécurité est appelé **état de sécurité de type association d'applications**. Il touche au contrôle de la sécurité des communications pour l'association d'applications considérée.
   - l'association de sécurité est appliquée sur une association d'objets ASO qui fait intervenir un transfert d'informations entre deux systèmes d'usager par l'intermédiaire d'un système de relais d'application – L'état de sécurité partagée se rapporte à la mise en œuvre de mécanismes de sécurité entre les deux systèmes d'usagers, indépendamment des mécanismes de sécurité utilisés dans les différentes associations d'applications établies avec un système de relais d'applications.

Exemples d'états de sécurité

a) informations d'état associées au chaînage cryptographique ou à la restauration de l'intégrité;

b) jeu d'étiquettes de sécurité associées aux informations pouvant être échangées;

c) clé(s) ou identification(s) de clés à utiliser pour fournir des services de sécurité dans les couches supérieures. Cela peut comprendre des clés pour des autorités de certification habilitées et connues (voir la Rec. X.509 du CCITT | ISO/CEI 9594-8: Annuaire – Cadre d'authentification), ou encore des clés permettant les communications avec un centre de distribution de clés;

d) identités authentifiées antérieurement;

e) numéros d'ordre et variables de synchronisation cryptographique.

L'état de sécurité peut être établi de diverses manières:

a) à l'aide d'une fonction de gestion de sécurité, auquel cas les informations d'état résident dans la base d'informations sur la gestion de la sécurité;

b) en tant qu'informations résiduelles provenant d'activités ou communication antérieures;

c) par des moyens extérieurs à l'OSI.

5.4 Exigences relatives à la couche application

Pour que des processus d'application puissent communiquer en toute sécurité, le contexte d'objet ASO (ou le contexte d'application) doit contenir les dispositions appropriées relatives à la sécurité.

Une définition de contexte d'objet ASO peut comprendre:

a) les types d'objets ASO et/ou les types d'éléments ASE requis pour prendre en charge les protocoles de sécurité;

b) des règles de négociation et de sélection des fonctions de sécurité relatives à la couche application et à la couche présentation;

c) des règles de sélection de services de sécurité sous-jacents;

d) des règles d'application de services particuliers de sécurité à des catégories spéciales d'informations à échanger;

e) des règles de réauthentification des identités concernées, pendant la durée de vie d'une association;

f) des règles de modification de clés pendant la durée de vie d'une association d'objets ASO (si des mécanismes fondés sur les techniques cryptographiques sont utilisés);

g) des règles à suivre en cas de défaillance des communications ou de détection de violations de la sécurité.

NOTE – On peut définir un contexte d'objet ASO par référence à la définition d'un type d'objet ASO.

Un contexte d'application est un cas particulier de contexte d'objet ASO qui décrit le comportement de communication autorisé de deux invocations d'objet ASO impliquées dans une association d'applications. Les aspects relatifs à la sécurité en 5.4.1 ci-dessus concernent les contextes d'application.

6 Architecture

6.1 Modèle général

La fourniture de services de sécurité OSI implique la création, l'échange et le traitement d'informations de sécurité conformément aux procédures de mécanismes de sécurité spécifiques. On distingue les deux types de fonction suivants:

a) *fonction de sécurité de système* – Capacité d'un système à accomplir des opérations liées à la sécurité telles que le chiffrement/déchiffrement, la signature numérique, ou bien la production ou le traitement d'un jeton de sécurité ou d'un certificat transmis dans un échange pour authentification. La réalisation de telles fonctions ne fait pas partie des services et protocoles de couche OSI:

b) *fonction de communication de sécurité* – Fonction prenant en charge le transfert d'informations relatives à la sécurité entre systèmes ouverts. Les fonctions de ce type sont mises en œuvre dans des entités d'application ou des entités de présentation OSI. Voici des exemples de fonctions de communication de sécurité:

- fonctions d'échange pour la sécurité, telles que décrites au 6.3;
- codage/décodage des éléments de protocole de la couche présentation conçus pour acheminer des informations chiffrées ou des informations de signature numérique;
- protocoles pour les communications avec un serveur de sécurité, par exemple service d'authentification ou centre de distribution de clés.

La distinction entre les fonctions de sécurité de système et les fonctions de communication de sécurité a une double importance. Le premier aspect est la distinction entre deux types de normes: en effet, les fonctions de sécurité-système sont spécifiées dans des normes relatives aux mécanismes ou aux techniques de sécurité. Ces normes sont généralement formulées en termes généraux et ne traitent pas nécessairement d'une couche ou d'un protocole de spécification particulier. Les normes relatives aux fonctions de sécurité de système peuvent avoir un domaine d'application autre que la sécurité des communications. En revanche, les fonctions de communication de sécurité font partie intégrante de spécifications particulières relatives aux protocoles de communication (par exemple couches supérieures OSI) et ne sont pas nécessairement liées à des mécanismes ou à des techniques de sécurité spécifiques.

Le deuxième aspect est la distinction entre la fonctionnalité de sécurité et la fonctionnalité de communication au stade de la mise en œuvre. Généralement, un ensemble de fonctions de sécurité de système est mis en œuvre sous la forme d'un module sécurisé (par exemple sous-système logiciel sécurisé ou module physique inviolable) susceptible d'être appliqué dans différents types de communications ou dans d'autres environnements. En conséquence, la distinction entre les fonctions de sécurité de système et les fonctions de communication de sécurité peut être un point de départ valable pour la définition d'interfaces applicatives normalisées (par exemple interfaces de programme d'application de sécurité).

A des fins d'architecture, il est nécessaire d'introduire le concept **d'objet de sécurité de système** (SSO). Un objet SSO représente un ensemble de fonctions de sécurité de systèmes connexes.

Pour fournir le ou les services de sécurité désirés les objets SSO peuvent interagir avec des fonctions de communication de sécurité via une limite (interface) avec le service abstrait. Les objets SSO produisent et traitent des information de sécurité échangées à l'aide de protocoles OSI dans les couches application et présentation. La structure logique de ces informations peut être normalisée dans l'OSI, pour qu'elles puissent être représentées dans les échanges protocolaires OSI.

Une invocation d'objet SSO représente une instance d'exécution d'un objet SSO. Dans un modèle dynamique, une invocation d'objet SSO peut interagir avec une invocation d'entité OSI, par exemple avec une invocation d'entité d'application.

Un objet SSO peut:

- accepter des informations provenant des fonctions de communication de sécurité OSI et leur en fournir, ces fonctions pouvant envoyer et/ou recevoir des informations au nom de l'objet SSO;
- provoquer l'établissement d'une association d'applications avec un autre système ouvert, un serveur d'authentification par exemple, et utiliser cette association d'applications pour fournir les fonctions de sécurité de système de l'objet SSO;
- établir une association de sécurité à utiliser ultérieurement lors de la fourniture d'un service de sécurité.

NOTE 1 – La définition de fonctions de sécurité de système, d'objets SSO ou de limites avec le service abstrait est en dehors du domaine d'application du présent Modèle de sécurité.

NOTE 2 – Des objets SSO peuvent être mis en œuvre à d'autres fins que la sécurité OSI. Toutefois, ces autres utilisations sont en dehors du domaine d'application du présent Modèle de sécurité.

La Figure 1 représente un modèle de base des fonctions de sécurité associées aux couches application et présentation. Dans ce modèle, les objets sont des entités d'application (AE), des entités de présentation (PE), des objets SSO et des services OSI qui les prennent en charge (dans les couches 1 à 5 de l'OSI). Ces services OSI fournissent l'infrastructure de communication de base permettant l'échange d'informations de sécurité (et d'informations non liées à la sécurité).

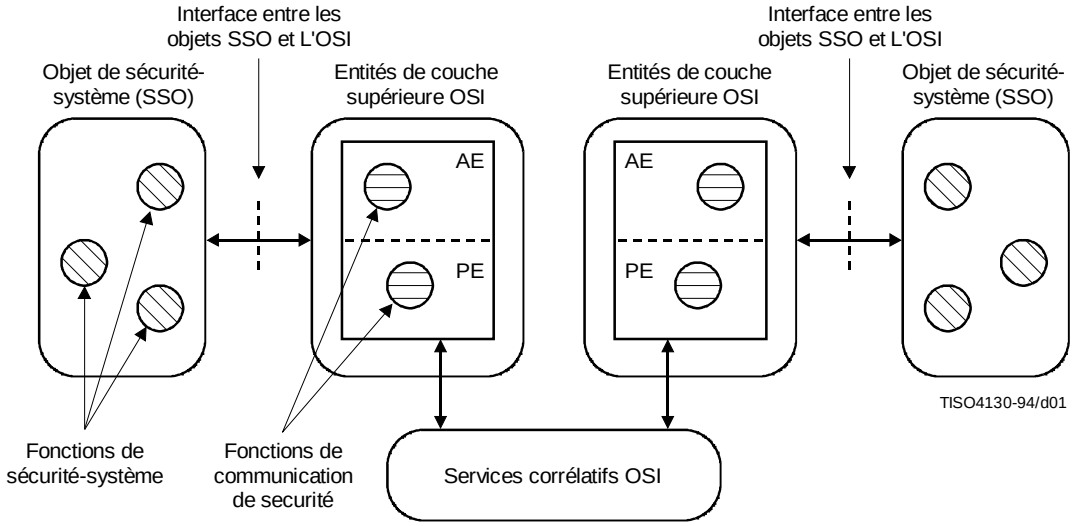

Figure 1 – Fonctions de sécurité liées aux couches supérieures OSI

Dans les couches supérieures, les entités de couche OSI contribuent à la fourniture de services de sécurité de la manière suivante:

- dans la couche application, les entités d'application représentent les aspects de communication des processus d'application et peuvent être structurées en éléments ASE, en objets ASO et en fonctions de contrôle (voir la Rec. X.207 du CCITT | ISO/CEI 9545). Une entité d'application peut contenir des éléments ASE et/ou des objets ASO dédiés à la fourniture de fonctions de communication de sécurité. Des éléments ASE et/ou objets ASO peuvent également permettre la protection des informations grâce aux transformations de sécurité (voir 6.4) et/ou en demandant aux couches inférieures une qualité de service appropriée;
- dans la couche présentation, c'est l'entité de présentation qui assure les fonctions de communication de sécurité. Ces fonctions peuvent collaborer avec les fonctions de sécurité de système (chiffrement par exemple) utilisées dans l'application d'une syntaxe abstraite sur une syntaxe de transfert (voir 6.4);
- dans la couche session, aucun service de sécurité n'est fourni. Cependant, 6.2.1 indique certains aspects du fonctionnement de la couche session qui peuvent avoir un impact sur la sécurité dans un environnement OSI.

Le modèle de base présenté ci-dessus facilite la définition générique des limites avec le service abstrait entre les composants OSI et les objets SSO; il permet également la fourniture de divers procédés d'habilitation (tels que les spécifie, par exemple, la Rec. UIT-T X.811 | ISO/CEI 10181-2).

NOTE 3 – Les interactions entre entités d'application et processus d'application, représentées à la Figure 1, sont traitées au 6.4 et au 8.1.

6.2 Associations de sécurité

Dans les couches supérieures, une association de sécurité est appliquée sur une association d'objets ASO. Le présent Modèle de sécurité ne donne aucune indication spécifique pour l'établissement ou la terminaison d'associations de sécurité. En règle générale, ces associations peuvent être établies/terminées conjointement avec les processus normalisés d'établissement d'association d'objets ASO ou par d'autres moyens. Des considérations architecturales particulières s'appliquent aux deux types particuliers d'associations de sécurité définis au 5.2.

6.2.1 Association de sécurité de type association d'applications

Une association de sécurité de type association d'applications est appliquée sur une association d'applications. Les services de sécurité peuvent être assurés à l'aide:

a) de fonctions de communication de sécurité dans la couche application et de fonctions de sécurité de système associées;

b) de fonctions de communication de sécurité dans la couche présentation et de fonctions de sécurité de système associées;

c) de services de sécurité fournis par les couches inférieures.

NOTE 1 – Comme l'indique la Rec. X.800 du CCITT | ISO 7498-2, aucun mécanisme de sécurité n'est fourni dans la couche session. Cependant, lors de la conception des protocoles de sécurité des couches supérieures, il faut tenir compte de deux aspects du fonctionnement de la couche session: le risque de non-remise des données (voir 8.2) qui découle de l'utilisation de services de session, et la réutilisation en série de connexions de transport afin de prendre en charge plusieurs connexions de session (voir 8.3).

Dans certains cas, la fourniture d'un service de sécurité peut nécessiter une combinaison de fonctions de communication de sécurité dans les couches application et présentation et de fonctions de sécurité de système associées.

Les services et les mécanismes de sécurité à utiliser dans le cadre d'une association d'applications sont définis par le contexte d'application. Ces services de sécurité peuvent être fournis par l'utilisation de fonctions associées à un ou à plusieurs éléments ASE et/ou d'objets ASO, séparément ou non.

Lors de l'établissement d'une association d'applications, il est nécessaire de tenir compte des exigences de sécurité relatives à cette association, de l'une des deux manières suivantes ou des deux:

a) via l'utilisation de services de sécurité destinés à protéger l'établissement de l'association d'applications;

b) via la sélection d'un contexte d'application comportant des services de sécurité appropriés.

Les services fournis par l'élément ACSE servent à établir une association d'applications et à sélectionner le contexte d'application approprié. Les règles du contexte d'application sélectionné peuvent comprendre des règles relatives à la sécurité. Ces règles peuvent exiger que d'autres éléments ASE capables de fournir des services de sécurité (entre autres services), fonctionnent conjointement avec l'élément ACSE pendant l'établissement de l'association.

NOTE 2 – Les fonctions de communication de sécurité dans la couche présentation et les fonctions de sécurité de système associées peuvent constituer une partie de la procédure d'établissement d'association d'applications.

L'état initial de sécurité d'association est déterminé par la procédure d'établissement d'association d'applications. Il peut dépendre de l'état de sécurité de système et/ou de l'état de sécurité d'association de toute association de sécurité établie. Les règles du contexte d'application peuvent permettre ou exiger des échanges protocolaires entre éléments ASE pour modifier cet état de sécurité d'association. De telles modifications peuvent survenir pendant les procédures d'initialisation qui suivent l'établissement de l'association d'applications et en tant que partie intégrante du fonctionnement normal d'invocations d'entité d'application coopérantes.

Pendant la durée de vie de l'association de sécurité, la modification de certains types d'informations d'état de sécurité peut être autorisée (numéros de séquences pour intégrité par exemple); la modification d'autres types d'informations d'état de sécurité peut être interdite (étiquettes de sécurité par exemple).

Les services fournis par l'élément ACSE sont utilisés pour terminer une association d'applications. Les règles du contexte d'application de l'association d'applications peuvent exiger que d'autres éléments ASE, capables de fournir des services de sécurité (entre autres services), fonctionnent conjointement avec l'élément ACSE pendant la terminaison de l'association d'applications.

6.2.2 Associations de sécurité par relais

Une association de sécurité par relais peut survenir dans une application répartie telle qu'une application en mode asynchrone, ou une application chaînée. Une association de sécurité par relais peut s'établir en même temps que des associations de sécurité de type association d'applications, comme le montre la Figure 2.

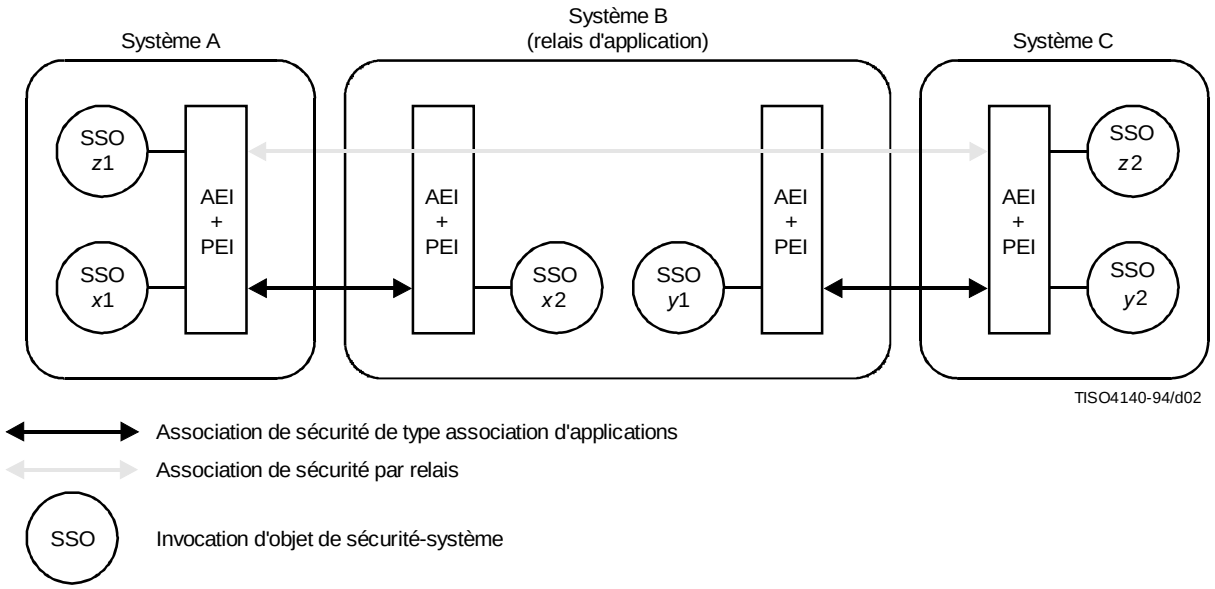

Figure 2 – Relais d'application (scénario)

Les informations relayées en mode protégé sont des informations transmises entre les correspondants d'une association de sécurité par relais (entre le système A et le système C sur la Figure 2). La protection est assurée à l'aide des fonctions de sécurité-système contenues dans les objets SSO *z*1 et *z*2. Ces informations relayées en mode protégé sont encastrées dans des valeurs PDV acheminées dans une association d'applications entre les systèmes A et B, d'une part, et dans les valeurs PDV acheminées dans une association d'applications entre les systèmes B et C, d'autre part. Lorsque des informations relayées en mode protégé sont acheminées dans une association d'applications, elles peuvent faire l'objet d'une protection de sécurité supplémentaire, par exemple au moyen des fonctions de sécurité dans les objets SSO *x*1 et *x*2, quand elles sont acheminées entre les systèmes A et B. C'est le cas notamment lorsqu'une valeur PDV, qui achemine des informations relayées en mode protégé, est elle-même encastrée dans une autre valeur PDV protégée au titre d'une association de sécurité de type association d'applications.

Il se peut que le système de relais d'application ne dispose pas des arguments (par exemple clés cryptographiques) permettant à l'entité ou aux entités de présentation du système ouvert de décoder/coder les valeurs PDV qui acheminent les informations relayées en mode protégé. Dans un système ouvert de ce type, les valeurs PDV codées peuvent être conservées et transmises ultérieurement. La transmission ultérieure est alors limitée à un contexte de présentation possédant la même syntaxe abstraite et la même syntaxe de transfert que le contexte dans lequel elles ont été reçues. D'où la nécessité de conserver les informations identifiant la syntaxe abstraite et la syntaxe de transfert, avec le codage, dans le système de relais.

La situation est similaire lorsque le système de relais possède les informations nécessaires au décodage des informations relayées. Par exemple, il peut disposer d'une clé publique qu'il utilise pour vérifier une signature associée à des informations (par exemple à l'appui d'une authentification de l'origine des données). Néanmoins, il peut être nécessaire de relayer les informations signées vers un autre système; dans ce cas, le codage doit être conservé de la façon décrite plus haut.

6.3 Fonctions d'échange pour la sécurité

Une fonction d'échange pour la sécurité est un type de fonction de communication de sécurité qui se trouve dans la couche application et qui permet de transmettre des informations relatives à la sécurité entre invocations d'entités d'application. A cet effet, la fonction d'échange pour la sécurité produit et traite des informations de contrôle de protocole d'application.

Les fonctions d'échange pour la sécurité sont fournies par les objets ASO ou par les éléments ASE.

Un exemple de ce type de fonction est le processus de communication relatif aux échanges pour authentification tel qu'il est décrit dans la Rec. UIT-T X.811 | ISO/CEI 10181-2, où un élément d'information d'authentification pour échange au niveau d'une invocation d'entité d'application de déclarant est transmis à une invocation d'entité d'application de vérificateur.

6.3.1 Echanges pour la sécurité

Un échange pour la sécurité représente le transfert d'informations de contrôle de protocole d'application entre des systèmes ouverts en tant que partie intégrante du fonctionnement d'un mécanisme de sécurité.

Un échange pour la sécurité peut impliquer:

a) le transfert d'une seule information entre deux systèmes ouverts, à savoir par exemple:
   - certificat de contrôle d'accès;
   - certificat de clé publique; ou
   - jeton de sécurité.

b) une séquence de transferts d'informations entre systèmes ouverts, la séquence complète faisant partie intégrante du fonctionnement d'un mécanisme de sécurité, à savoir par exemple:
   - transferts d'informations associés à un échange d'authentification bi ou trilatéral; ou
   - négociation bilatérale de clé de session (par exemple échange avec clé exponentielle Diffie-Hellman[2)].

On attribue des identificateurs uniques à différents types d'échanges pour la sécurité afin d'en indiquer l'utilisation dans les protocoles.

6.3.2 Informations d'échange pour la sécurité

Les informations d'échange pour la sécurité sont les informations transmises entre des systèmes ouverts lors d'un échange pour la sécurité.

On appelle **item d'échange pour la sécurité** (SEI) une portion d'information, distincte logiquement, qui correspond à un transfert donné (éventuellement dans une série de transferts). Pour la définition des données, un item SEI est décomposable en éléments de taille inférieure.

---

2) DIFFIE (W.), HELLMAN (M.): New Directions in Cryptography, *IEEE Transactions on Information Theory*, Vol. IT-22, n° 6, pp. 644-654, 1976.

Bien qu'aucune notation de syntaxe abstraite particulière ne soit stipulée en vue de définir des informations d'échange pour la sécurité, la création d'une syntaxe abstraite complète contenant ce type d'informations sera facilitée si on utilise pour ces informations la même notation que pour le reste de la syntaxe abstraite. La Rec. UIT-T X.830 | ISO/CEI 11586-1 décrit les principes de notation à utiliser en notation ASN.1.

6.3.3 Fourniture des fonctions d'échange pour la sécurité

Afin qu'un échange pour la sécurité puisse être pris en charge dans n'importe quel contexte d'objet ASO, la fonction correspondante doit être intégrée dans certains éléments ASE et/ou objets ASO appartenant à ce contexte d'objet ASO. Ceci comprend:

a) l'incorporation des définitions des types d'item SEI dans une syntaxe abstraite;

b) l'incorporation de toute règle procédurale ou autre concernant le fonctionnement de l'échange pour la sécurité dans la définition du type d'élément ASE ou d'objet ASO, ou à tout autre endroit dans la définition du contexte d'objet ASO.

c) si nécessaire, l'incorporation de la définition de règles de coordination concernant l'échange pour la sécurité dans la spécification d'une fonction CF.

En général, les échanges pour la sécurité peuvent être incorporés dans n'importe quel élément ASE et/ou objet ASO. D'autre part, les définitions d'item SEI devraient être exprimées de manière à faciliter leur incorporation dans le plus grand nombre d'éléments ASE et/ou d'objets ASO possible.

Les Rec. UIT-T X.831 | ISO/CEI 11586-2 et UIT-T X.832 | ISO/CEI 11586-3 définissent un élément ASE conçu spécifiquement en vue d'assurer les échanges pour la sécurité.

6.4 Transformations pour la sécurité

Une transformation pour la sécurité est un ensemble de fonctions (fonctions de sécurité de système et de communication de sécurité) qui, par un effet de combinaison, assure la protection des éléments de données d'utilisateur dans des conditions spécifiques pendant la communication ou la mémorisation.

Les transformations pour la sécurité concernent le traitement, lié à la sécurité, des informations d'utilisateur acheminées par les protocoles des couches supérieures OSI. Elles peuvent constituer le principal moyen de fournir des services de confidentialité, d'intégrité, ou d'authentification de l'origine des données et/ou contribuer à la fourniture d'autres services de sécurité tels que les services d'authentification d'entité, de contrôle d'accès et de non-répudiation.

Les transformations pour la sécurité font appel à des fonctions de sécurité de système de plusieurs types, telles que les suivantes:

a) les fonctions de chiffrement/déchiffrement (par exemple pour les services de confidentialité);

b) les fonctions de signature ou de scellement (par exemple pour les services d'intégrité ou d'authentification de l'origine des données).

Une transformation pour la sécurité peut faire appel à une seule fonction de sécurité de système ou à différentes fonctions de ce type, utilisées conjointement. Lorsque ces fonctions sont appliquées en combinaison, aucune restriction d'ordre architectural n'est imposée quant à l'ordre dans lequel elles doivent être appliquées.

Les transformations pour la sécurité utilisent également des fonctions de communications de sécurité, situées dans les couches supérieures.

NOTE 1 – Les exemples a) et b) ci-dessus ne constituent pas une liste exhaustive des types de fonctions de sécurité-système.

NOTE 2 – Il est souhaitable de limiter le nombre des types de fonctions de sécurité-système définis et de les appliquer à une large gamme de besoins de sécurité.

NOTE 3 – Les fonctions de communication de sécurité qui font partie intégrante des transformations pour la sécurité portent sur des représentations d'informations: logiquement, elles sont donc associées à la couche présentation, mais leur application correspond à différents niveaux de granularité; elles peuvent s'appliquer à des valeurs PDV intégrales telles que reconnues par le protocole de présentation ou à des portions spécifiques des informations de couche application. Dans ce dernier cas, il peut être plus commode, du point de vue de la mise en œuvre, de considérer que les fonctions de communication de sécurité appartiennent à la couche application.

On attribue des identificateurs uniques à différents types de transformations pour la sécurité afin d'en indiquer l'utilisation dans les protocoles.

Il est possible qu'une spécification concernant l'utilisation de transformations pour la sécurité ait besoin d'inclure:

a) une indication de la transformation pour la sécurité considérée ou des moyens qui permettront de déterminer cette transformation;

b) la spécification de l'élément ou des éléments d'information auxquels la transformation pour la sécurité doit s'appliquer;

c) éventuellement, une indication des règles de codage/décodage à utiliser avant/après l'application d'une transformation pour la sécurité si un élément d'information à protéger est spécifié dans un niveau de la syntaxe abstraite;

d) une indication de l'algorithme ou des algorithmes à utiliser ainsi que de la source de tout paramètre requis (par exemple, clés).

NOTE 4 – Les règles de codage/décodage utilisées pour produire/vérifier les valeurs de contrôle d'intégrité ou les signatures numériques doivent toujours avoir pour propriété qu'il y ait une relation bijective entre la valeur abstraite des informations et leur valeur codée. Les règles de codage distinctives et canoniques pour l'ASN.1 possèdent cette propriété, contrairement aux règles de codage de base pour l'ASN.1.

Deux méthodes permettent de spécifier les éléments d'information auxquels s'appliquent les transformations pour la sécurité:

a) indication des champs sélectionnés dans une spécification de syntaxe abstraite;

b) association d'une transformation pour la sécurité d'un type particulier à tous les éléments d'information transférés dans un contexte de présentation; en l'occurrence, les exigences relatives à la transformation pour la sécurité ne font pas partie intégrante de la spécification de syntaxe abstraite.

Ces deux possibilités sont décrites en détail dans la suite du texte.

6.4.1 Indication sélective des champs dans une spécification de syntaxe abstraite

Lorsque la protection s'applique à des champs particuliers en syntaxe abstraite, la spécification de cette syntaxe doit indiquer les éléments à protéger à l'aide d'une notation appropriée. On doit utiliser cette méthode si la confidentialité sélective et/ou l'intégrité des champs s'appliquent avec une granularité inférieure à celle des valeurs PDV intégrales produites par une syntaxe abstraite.

A titre d'exemples illustrant la notation qui permet de spécifier l'utilisation sélective des transformations pour la sécurité dans une syntaxe abstraite, on peut citer les fonctions de signature et de chiffrement définies dans la Rec. UIT-T X.509 | ISO/CEI 9594-8 et la notation PROTEGÉE définie dans la Rec. UIT-T X.830 | ISO/CEI 11586-1.

6.4.2 Contextes de protection de la présentation

Lorsqu'une transformation pour la sécurité doit s'appliquer uniformément à tous les éléments d'information d'une syntaxe abstraite, il est nécessaire d'établir et d'utiliser un **contexte de protection de la présentation**.

L'établissement d'un tel contexte nécessite la mise en place d'une syntaxe de transfert destinée à être utilisée avec une syntaxe abstraite déterminée. Dans le cas d'un contexte de protection de la présentation, la syntaxe de transfert, appelée **syntaxe de protection du transfert**, repose sur des processus de codage/décodage faisant appel à une transformation pour la sécurité. Mettre en place un contexte de protection de la présentation revient notamment à déterminer la transformation pour la sécurité ainsi que la ou les fonctions de sécurité-système associées qui feront partie intégrante des processus de codage/décodage entre la syntaxe abstraite et la syntaxe de transfert à l'émission/réception de toutes les valeurs PDV de ce contexte de présentation.

Une fois un contexte de protection de la présentation établi, il se peut que la fonction de sécurité-système qui traite les données sortantes ait à acheminer des informations paramétriques vers la fonction de sécurité-système correspondante. Ces informations peuvent comprendre, par exemple:

a) lors de la première utilisation du contexte de présentation, des paramètres initiaux tels que le vecteur d'initialisation d'un processus cryptographique, ou encore l'identificateur ou les identificateurs de clés;

b) dans une série de valeurs PDV protégées, des informations signalant une modification de paramètre, une nouvelle clé par exemple.

En conséquence, il se peut que la définition d'une syntaxe de protection du transfert doive contenir les moyens d'acheminer des données paramétriques de transformation en plus des représentations des informations d'utilisateur du service de présentation.

Les informations paramétriques (clés, par exemple), requises par les fonctions de sécurité-système, peuvent être obtenues à l'aide de moyens tels que les suivants:

a) le résultat d'échanges protocolaires antérieurs de la couche application, une clé provenant, par exemple, d'un échange pour sécurité de calcul de clé:

b) par des moyens locaux, par exemple l'insertion manuelle de clés.

La Rec. UIT-T X.833 | ISO/CEI 11586-4 spécifie une syntaxe générique de protection du transfert pouvant supporter différentes transformations pour la sécurité.

NOTE – Il est possible d'encastrer une valeur PDV dans une autre valeur PDV, les transformations pour la sécurité pouvant s'appliquer au niveau des deux valeurs. En l'occurrence, le codage de la valeur PDV interne (encastrée) – qui fait intervenir une transformation pour la sécurité – sera également protégé dans le cadre de la transformation pour la sécurité applicable au codage de la valeur PDV externe. On pourrait par exemple citer le cas où l'authentification de l'origine des données (comprenant une valeur PDV interne) acheminées entre deux systèmes nécessite une signature et où la protection contre les attaques par réexécution entre les deux systèmes est obtenue par application d'un sceau à une valeur PDV externe ou bien à l'ensemble des valeurs PDV dans un contexte de présentation.

7 Services et mécanismes

L'architecture de sécurité OSI (Rec. X.800 du CCITT | ISO 7498-2) spécifie:

– que la couche application peut fournir un ou plusieurs des services de sécurité de base: authentification, contrôle d'accès, confidentialité, intégrité de données et non-répudiation;

– que la couche présentation ne fournit pas de service de sécurité mais que des mécanismes de sécurité permettant la prise en charge de services de sécurité de la couche application peuvent y être localisés;

– que la couche session ne fournit aucun service de sécurité et ne contient aucun mécanisme de sécurité.

7.1 Authentification

7.1.1 Authentification d'entité

7.1.1.1 Rôle des couches supérieures dans l'authentification d'entité

L'authentification a pour but de garantir l'identité d'une entité. C'est le rôle de la couche application d'authentifier les entités connues d'elle. Cette authentification s'effectue au moment de l'établissement de l'association d'objets ASO et pendant son utilisation.

La couche application permet l'authentification d'une large gamme d'entités principales. Cela dépend de la nature de l'application et de la politique de sécurité en vigueur.

NOTE – Le concept d'*authentification de l'entité homologue* défini dans la Rec. X.800 du CCITT | ISO 7498-2 est un cas particulier d'*authentification d'entité* telle que la définit la Rec. UIT-T X.811 | ISO/CEI 10181-2.

Les couches supérieures ne permettent pas l'authentification d'entités situées au-dessous de la couche application.

7.1.1.2 Fourniture de l'authentification d'entité

L'authentification d'entité peut être fournie dans la couche application par communication d'informations d'authentification pour échange pouvant faire appel à des fonctions d'échange pour la sécurité conformément au 6.3.

L'authentification d'entité ne garantit une identité qu'à un moment donné. Pour que cette garantie coure pendant toute la durée d'une association d'objets ASO, il est nécessaire de mettre en œuvre un service d'intégrité en mode connexion (défini dans la Rec. X.800 du CCITT | ISO 7498-2). Dans certains cas, il peut être nécessaire, au bout d'un certain temps, d'obtenir une garantie supplémentaire de l'identité d'une entité par d'autres échanges pour authentification.

7.1.1.3 Gestion de l'authentification d'entité

Lorsqu'un service d'authentification d'entité est fourni, la gestion des informations d'authentification pour déclaration et/ou des informations d'authentification pour vérification, telles que les clés cryptographiques, peut s'avérer nécessaire. Comme le décrit la Rec. UIT-T X.811 | ISO /CEI DIS 10181-2, cela peut impliquer les procédures suivantes:

– *installation:* les informations d'authentification pour déclaration et pour vérification sont définies;

– *modification des informations d'authentification:* un gestionnaire ou une entité principale provoque la modification des informations d'authentification pour déclaration et pour vérification;

- *distribution:* toute entité peut obtenir assez d'informations d'authentification pour vérification afin de vérifier des informations d'authentification pour échange;
- *invalidation:* établissement d'un état rendant temporairement impossible l'authentification d'une entité auparavant authentifiable;
- *réactivation:* fin de l'état établi par la procédure de désactivation;
- *désinstallation:* une entité principale est retirée de l'ensemble d'entités principales authentifiables.

La mise en œuvre de ces procédures à l'aide de protocoles OSI peut faire appel à des fonctions d'échange pour la sécurité, conformément au 6.3. Ces procédures peuvent également utiliser des services de gestion de sécurité OSI.

La politique de sécurité en vigueur peut également exiger que toute tentative d'authentification rejetée soit signalée afin de déclencher une alarme et/ou de l'enregistrer dans un journal d'audit de sécurité.

7.1.2 Authentification de l'origine des données

7.1.2.1 Rôle des couches supérieures dans l'authentification de l'origine des données

L'authentification de l'origine des données concerne l'authentification de l'entité qui est déclarée source d'un ensemble particulier de données. Comme cette entité n'est pas nécessairement l'entité homologue dans une instance de communication, l'authentification de l'origine des données n'a pas le même objectif que l'authentification d'entité.

Chaque élément de données d'une instance de communication peut être, ou non, soumis à l'authentification de l'origine des données. Afin d'assurer l'à-propos des données reçues, il peut être nécessaire que l'authentification de l'origine puisse valider l'heure de leur émission aussi bien que l'entité source.

7.1.2.2 Fourniture de l'authentification de l'origine des données

Dans la couche application, l'authentification de l'origine des données est fournie par l'échange d'informations de sécurité qui peuvent acheminer, par exemple, une signature numérique fondée sur les données et sur un identificateur de l'origine des données. L'authentification de l'origine des données peut être fournie soit au moment de l'établissement de l'association d'objets ASO ou à tout autre moment de cette association.

Les services d'authentification de l'origine des données utilisent des transformations de sécurité utilisant généralement des mécanismes de chiffrement ou de signature numérique.

7.1.2.3 Gestion de l'authentification de l'origine des données

La gestion de l'authentification de l'origine des données est, en principe, la même que la gestion de l'authentification d'entité (voir 7.1.1.3).

7.2 Contrôle d'accès

7.2.1 Considérations générales

Les protocoles de la couche application peuvent assurer l'échange d'informations de contrôle d'accès, par exemple un certificat de contrôle d'accès, c'est-à-dire des informations concernant l'attribution, la mise en application et/ou la révocation des droits de contrôle d'accès.

Les informations de contrôle d'accès peuvent être échangées soit au moment de l'établissement de l'association d'objets ASO, ou à tout autre moment de cette association. Les droits d'accès présentés au cours d'une association d'objets ASO peuvent soit modifier (accroître ou réduire) les droits valides pendant le reste de cette association, ou n'être valides que pour une demande spécifique.

Le contrôle d'accès peut être appliqué à différents niveaux de granularité. On distingue deux niveaux, le niveau association d'objets ASO et le niveau ressource. Cependant, des protocoles particuliers peuvent introduire des niveaux supplémentaires dans la catégorie ressource.

7.2.2 Contrôle d'accès au niveau association d'objets ASO

7.2.2.1 Rôle des couches supérieures dans le contrôle d'accès au niveau association d'objets ASO

Le contrôle d'accès au niveau association d'objets ASO s'applique au niveau de l'association en question; il concerne le contrôle d'accès aux systèmes et aux processus (par exemple aux processus d'application) plutôt qu'aux objets contenus dans les systèmes. Son but est d'établir si l'association d'objets ASO demandée à partir d'un système distant donné, avec le contexte d'objets ASO et les caractéristiques de sécurité requis, est autorisée à démarrer ou à continuer si son utilisation est postérieure à l'établissement de l'association d'objets ASO.

7.2.2.2 Fourniture du contrôle d'accès au niveau association d'objets ASO

Le contrôle d'accès au niveau association d'objets ASO peut être pris en charge par des fonctions d'échange pour la sécurité telles que décrites au 6.3. Ces fonctions peuvent supporter plusieurs des classes de mécanisme identifiées dans la Rec. UIT-T X.812 | ISO/CEI 10181-3: Cadre de contrôle d'accès.

Une telle fonction d'échange pour la sécurité peut être fournie par un élément ASE utilisé conjointement avec l'élément ACSE pour assurer le contrôle d'accès au moment de l'établissement de l'association applicative. De plus, un échange pour la sécurité à ce moment-là permet de conserver certaines informations relatives au contrôle d'accès pour une utilisation ultérieure, en prenant des décisions concernant le contrôle de l'accès pendant la durée de vie de l'association d'applications.

7.2.2.3 Gestion du contrôle d'accès au niveau association d'objets ASO

La politique de sécurité en vigueur dans un système peut exiger que toutes les tentatives d'accès, plus particulièrement celles qui sont rejetées, soient signalées afin de déclencher une alarme et/ou d'être enregistrées dans un journal d'audit de sécurité. Les services de gestion de sécurité OSI fournissent les moyens de conserver les informations relatives au contrôle d'accès.

7.2.3 Contrôle d'accès au niveau ressource

7.2.3.1 Rôle des couches supérieures dans le contrôle d'accès au niveau ressource

Le contrôle d'accès au niveau ressource concerne le contrôle de l'accès à une ressource donnée: par exemple à des objets d'informations ou à des objets d'une base d'informations. Lorsqu'un objet est organisé en plusieurs parties, des niveaux supplémentaires de contrôle d'accès peuvent être fournis. Un fichier est un exemple de ce genre de ressource. Le contrôle d'accès peut servir à déterminer si l'utilisateur est autorisé à effectuer une opération particulière sur le fichier (par exemple lecture ou modification).

7.2.3.2 Fourniture du contrôle d'accès au niveau ressource

Le contrôle d'accès au niveau ressource peut être du domaine de l'élément ASE ou de l'objet ASO qui fournit le protocole d'échange de demandes et de réponses de manipulation pour une ressource donnée. Ainsi, par exemple, le contrôle d'accès aux fichiers est du domaine du transfert, de l'accès et de la gestion de fichiers (FTAM) (ISO 8571).

Ces éléments ASE peuvent faire appel à une ou à plusieurs des classes de mécanismes définies dans la Rec. UIT-T X.812 | ISO/CEI 10181-3. Ils peuvent également faire appel à des informations de contrôle d'accès conservées suite à l'utilisation du contrôle d'accès au niveau association d'objets ASO.

7.2.3.3 Gestion du contrôle d'accès au niveau ressource

La politique de sécurité en vigueur dans un système peut exiger que toutes les tentatives d'accès, plus particulièrement les tentatives rejetées, soient signalées afin de déclencher une alarme et/ou d'être enregistrées dans un journal d'audit de sécurité. La gestion des informations relatives au contrôle d'accès peut être effectuée via le protocole spécifique à l'application ou via un protocole général de gestion de la couche application.

7.3 Non-répudiation

7.3.1 Rôle des couches supérieures dans la non-répudiation

La non-répudiation est un service de la couche application qui couvre les cas suivants (définis dans la Rec. X.800 du CCITT | ISO 7498-2) sans se limiter à eux:

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

b) non-répudiation avec preuve de la remise.

Dans le cas de la non-répudiation avec preuve de l'origine, le destinataire des données reçoit la preuve de leur origine. Cela protège contre toute tentative ultérieure de l'expéditeur de nier l'envoi de ces informations. Le rôle des couches supérieures dans la non-répudiation avec preuve de l'origine est de fournir la preuve qu'un élément particulier d'information a été envoyé par une entité d'application donnée.

Dans le cas de la non-répudiation avec preuve de la remise, l'expéditeur des données reçoit la preuve de leur remise au destinataire. Cela protège contre toute tentative ultérieure du destinataire de nier la réception des données. Le rôle des couches supérieures dans la non-répudiation avec preuve de la remise est de fournir la preuve qu'un élément d'information donné a été reçu par une entité d'application donnée.

7.3.2 Fourniture de la non-répudiation

La fourniture des services de non-répudiation repose sur des mécanismes de signature numérique ou de chiffrement. Cela peut comporter l'utilisation de transformations de sécurité telles que définies au 6.4. Selon la politique de sécurité en vigueur, les services de non-répudiation peuvent faire appel à un mécanisme de notarisation.

Une interaction avec un tiers habilité peut être nécessaire dans le cas de la non-répudiation avec preuve de l'origine. Elle l'est toujours dans le cas de la non-répudiation avec preuve de la remise.

L'expéditeur et/ou le destinataire peuvent être amenés à utiliser plusieurs associations d'objets ASO pour leurs interactions avec, par exemple, un service de création de signatures, un service d'horodatage et/ou un service de répertoire.

7.3.3 Gestion de la non-répudiation

Si des mécanismes de signature numérique et/ou de chiffrement sont utilisés pour fournir un service de non-répudiation, leur gestion peut comprendre:

- la gestion de clé; et
- l'établissement de paramètres et d'algorithmes cryptographiques.

Si un mécanisme de notarisation est utilisé pour fournir un service de non-répudiation, sa gestion peut comprendre:

- la distribution d'informations relatives aux notaires; et
- l'interaction avec les notaires.

7.4 Intégrité

7.4.1 Rôle des couches supérieures dans l'intégrité des données

L'intégrité des données peut être un service de la couche application. La fourniture de ce service peut utiliser des fonctions de communication de sécurité dans la couche présentation et des fonctions de sécurité-système associées. Les services suivants peuvent être fournis:

a) intégrité en mode connexion avec restauration;

b) intégrité en mode connexion sans restauration;

c) intégrité en mode connexion sélective par champ;

d) intégrité en mode sans connexion;

e) intégrité en mode sans connexion sélective par champ.

Tous les types de services d'intégrité, à l'exception de l'intégrité sélective par champ, peuvent être fournis par les couches inférieures.

En principe, l'intégrité peut être appliquée selon un des niveaux de granularité suivants:

a) à une valeur PDV individuelle;

b) à une série de valeurs PDV du même contexte de présentation;

c) à une partie, ou à plusieurs parties, d'une valeur PDV individuelle.

7.4.2 Fourniture de l'intégrité de données

Les services d'intégrité de données peuvent être fournis en utilisant des transformations de sécurité telles que décrites au 6.4.

La détection d'une violation d'intégrité dans la couche présentation est signalée par une indication à l'entité d'application destinataire. Toutefois, il n'est pas possible d'analyser la donnée reçue ni de la mettre explicitement à la disposition de l'utilisateur du service de présentation. Néanmoins, la donnée suspecte devrait être disponible à des fins d'analyse/d'audit dans le système ouvert destinataire. Selon les résultats de cette analyse, d'autres actions connexes dans l'environnement OSI peuvent être appelées.

7.4.3 Gestion de l'intégrité des données

La gestion de l'intégrité des données peut comporter la communication d'informations sur les clés. Lorsque cette communication survient dans une association d'objets ASO (peut-être la même association d'objets ASO que celle dans laquelle le service d'intégrité est utilisé), elle peut utiliser des fonctions d'échange pour la sécurité conformément au 6.3. La communication de certaines informations sur les clés peut comporter une application de sécurité et/ou des services de gestion de sécurité OSI.

7.5 Confidentialité

7.5.1 Rôle des couches supérieures dans la confidentialité

La confidentialité peut être fournie par un service de la couche application. La fourniture de ce service peut utiliser des fonctions de communication de sécurité dans la couche présentation et des fonctions de sécurité-système associées. Les services suivants peuvent être fournis:

a) confidentialité en mode connexion;

b) confidentialité en mode sans connexion;

c) confidentialité sélective par champ;

d) confidentialité des flux de trafic.

Tous les types de services de confidentialité, à l'exception de la confidentialité sélective par champ, pourront être fournis dans les couches inférieures.

En principe, la confidentialité peut s'appliquer aux niveaux suivants:

– à une valeur PDV individuelle;

– à une série de valeurs PDV du même contexte de présentation;

– à une partie, ou à plusieurs parties, d'une valeur PDV.

7.5.2 Fourniture de la confidentialité

Les services de confidentialité peuvent être fournis en utilisant des transformations pour sécurité telles que décrites au 6.4.

7.5.3 Gestion de la confidentialité

La gestion de la confidentialité peut comporter la communication d'informations sur les clés. Lorsque cette communication survient dans une association d'objets ASO (peut-être la même que celle dans laquelle le service de confidentialité est utilisé), elle peut utiliser des fonctions d'échange pour la sécurité conformément au 6.3. La communication de certaines informations sur les clés peut comporter une application de sécurité et/ou des services de gestion de sécurité OSI.

8 Interactions entre couches

8.1 Interactions entre la couche application et la couche présentation

8.1.1 Invocation de transformations pour la sécurité

Au moment de l'établissement d'un contexte de présentation, il est possible de spécifier, par des moyens locaux, l'application d'une transformation pour sécurité aux valeurs PDV transférées selon ce contexte de présentation. Le 6.4.2 donne une description détaillée des contextes de présentation de protection.

L'utilisation de transformations pour la sécurité peut aussi découler de la notation dans une spécification de syntaxe abstraite. Le 6.4.1 donne des renseignements détaillés à ce sujet.

Lorsqu'une valeur PDV à laquelle est appliquée la transformation possède des valeurs PDV encastrées, la transformation leur est également appliquée à ces valeurs de présentation.

La détection d'une violation d'intégrité est signalée sous la forme d'une indication à l'entité d'application destinataire.

8.1.2 Informations requises par la couche présentation

L'entité de présentation initiatrice obtient l'identité d'une transformation requise pour la sécurité de la part de la base d'informations sur la gestion-sécurité ou, implicitement, de la part de la syntaxe de transfert utilisée pour un contexte de présentation.

Les paramètres de transformation pour la sécurité, y compris les clés de chiffrement, peuvent être obtenus, par des moyens locaux, à partir des informations contenues dans la base d'informations sur la gestion-sécurité, ou bien ils peuvent être déterminés par des échanges de données encastrés dans une syntaxe de protection du transfert. En outre, les informations paramétriques peuvent être transmises dans d'autres valeurs PDV en mode protégé au titre de la même association d'objets ASO. La détermination des valeurs paramétriques peut nécessiter l'utilisation de divers attributs de connexion, y compris les identités des points d'accès au service de présentation du côté initiateur et du côté répondeur.

NOTE – Ces informations peuvent comprendre des données relatives aux états ou aux séquences. Il peut s'avérer nécessaire de faire modifier ces informations par des fonctions de sécurité-système.

8.1.3 Aspects des applications réparties

Certaines applications réparties, telles que les applications en mode asynchrone ou chaînées, nécessitent des unités de données protocolaires d'application ou des parties de ces unités, pour traverser un système ouvert faisant fonction de relais d'application (voir 6.2.3). Dans un système à relais d'application de ce genre, les valeurs PDV codées peuvent être conservées pour émission ultérieure. Cette émission devra être limitée à un contexte de présentation ayant la même syntaxe abstraite et la même syntaxe de transfert que le contexte de réception de ces valeurs PDV.

8.2 Interactions entre la couche présentation et la couche session

Si la couche session ne comporte aucun service ou mécanisme de sécurité, des opérations internes à cette couche peuvent avoir un effet sur le fonctionnement de certains mécanismes de sécurité de la couche présentation. En particulier, le fonctionnement de certains services destructifs de la couche session, tels que la resynchronisation (qui rejette des données), aura un effet sur le fonctionnement des mécanismes de chiffrement et sur la prise en charge de l'intégrité des données dans la couche présentation. Cette couche peut contenir des procédures permettant de contrecarrer ces effets.

Ainsi, par exemple, en cas de resynchronisation de session, il pourra être nécessaire de resynchroniser également les processus de chaînage cryptographique (supportant par exemple des services d'intégrité) dans la couche présentation.

8.3 Utilisation des services des couches inférieures

Des règles d'interaction sécurisées peuvent nécessiter la protection des communications OSI par l'utilisation de caractéristiques de sécurité dans les couches inférieures. Ces caractéristiques pourront s'ajouter aux mesures de sécurité des couches supérieures ou les remplacer.

Les services de sécurité des couches inférieures peuvent fournir une protection que les couches supérieures ne peuvent pas assurer. En particulier, les services de sécurité des couches inférieures peuvent servir à protéger toutes les informations de contrôle de protocole des couches supérieures et fournir un degré de confidentialité plus élevé du flux de données.

L'identification des besoins en caractéristiques de sécurité fournies par le service de transport est décrite dans la Rec. X.214 du CCITT | ISO 8072 par le paramètre protection des connexions de transport, qui est un paramètre de qualité du service de protection , lequel fait partie du service d'établissement de la connexion de transport. Ce paramètre permet de transmettre les besoins en services de sécurité entre un utilisateur du service de transport et un fournisseur du service de transport.

La sélection des caractéristiques de sécurité du service de transport (au moyen du paramètre protection des connexions de transport) peut être déterminée, entièrement ou partiellement, par gestion-système locale, plutôt que par protocoles de couches supérieures.

NOTE – La notion de qualité du service de protection est actuellement à l'étude. elle pourra être modifiée (voire supprimée) dans les normes relatives aux couches inférieures, d'ici à la prochaine révision de la présente norme.

Annexe A

Relation avec la gestion OSI

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

A.1 Gestion des services et mécanismes de sécurité

Les services de gestion de sécurité OSI peuvent être utilisés pour gérer les services et les mécanismes de sécurité. La gestion des services de sécurité concerne la gestion de services de sécurité particuliers tels l'authentification d'entité et le contrôle d'accès. Les services de sécurité sont fournis par l'utilisation d'un ou de plusieurs mécanismes de sécurité; la gestion des mécanismes de sécurité concerne leur analyse et leur contrôle.

Les activités de gestion de la sécurité sont généralement les suivantes:

a) gestion de la politique de sécurité;

b) interactions entre fonctions de sécurité et d'autres fonctions OSI (par exemple gestion de configuration);

c) interactions entre les fonctions de gestion de services de sécurité et les fonctions de gestion de mécanismes de sécurité;

d) gestion de la signalisation des alarmes de sécurité et des pistes de vérification de sécurité;

e) gestion des informations de contrôle d'accès.

A.2 Objets, attributs et rapports d'événement pour la sécurité

La gestion OSI fournit des fonctions qui permettent de gérer des objets et attributs relatifs à la sécurité, et de produire des rapports d'événement liés à la sécurité. Ces objets, attributs et rapports d'événement comprennent:

a) les rapports d'événement relatifs aux alarmes de sécurité, tels que définis dans la Rec. X.736 du CCITT | ISO/CEI 10164-7;

b) les objets, attributs et rapports d'événement relatifs aux pistes de vérification de sécurité, tels que définis dans la Rec. X.740 du CCITT | ISO/CEI 10164-8;

c) les objets et attributs relatifs au contrôle d'accès pour la gestion OSI, tels que définis dans la Rec. UIT-T X.741 | ISO/CEI 10164-9.

A.3 Fonctions spécifiques de gestion de sécurité

La gestion des entités dans chaque couche OSI peut produire des rapports, à la suite de la détection d'attaques et de risques signalant des événements normaux et anormaux, y compris l'activation ou la désactivation du service. Les aspects de gestion de traitement d'événements dans l'OSI comprennent la notification à distance de tentatives apparentes de violer la sécurité de système ou la notification d'événements. La fonction de signalisation des alarmes de sécurité définie dans la Rec. X.736 du CCITT | ISO/CEI 10164-7 supporte ces caractéristiques.

La gestion de vérification de sécurité comprend certains aspects d'enregistrement et/ou de collecte à distance d'informations de vérification sur des événements sélectionnés, la collecte à distance d'enregistrement de vérification choisis et la préparation de rapports de vérification de sécurité. La fonction de piste de vérification de sécurité définie dans la Rec. X.740 du CCITT | ISO/CEI 10164-8 supporte ces spécifications.

A.4 Autres aspects de la gestion de sécurité

Des objets associés à la sécurité peuvent être créés et supprimés; leurs attributs peuvent être manipulés grâce à la fonction de gestion d'objets spécifiée dans la Rec. X.730 du CCITT | ISO/CEI 10164-1. Il est possible par exemple de créer des listes de contrôle d'accès et de gérer les informations de sécurité qu'elles contiennent.

La fonction de gestion de relations, spécifiée dans la Rec. X.732 du CCITT | ISO/CEI 10164-3, peut gérer les relations entre les objets qui représentent les applications OSI et les objets liés à la sécurité.

Annexe B

Bibliographie

(Cette annexe ne fait pas partie intégrante de la présente Recommandation | Norme internationale)

- Recommandation UIT-T X.509 (1993) | ISO/CEI 9594-8, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: Cadre d'authentification.*
- Recommandation X.730 du CCITT (1992) | ISO/CEI 10164-1:1993, *Technologies de l'information – Interconnexion de systèmes ouverts – Gestion des systèmes: Fonction de gestion des objets.*
- Recommandation X.732 du CCITT (1992) | ISO/CEI 10164-3:1993, *Technologie de l'information – Interconnexion de systèmes ouverts – Gestion des systèmes. Attributs relationnels.*
- Recommandation X.736 du CCITT (1992) | ISO/CEI 10164-7:1992, *Technologie de l'information – Interconnexion de systèmes ouverts – Gestion des systèmes: Fonction de signalisation des alarmes de sécurité.*
- Recommandation X.740 du CCITT (1992) | ISO/CEI 10164-8:1993, *Technologie de l'information – Interconnexion de systèmes ouverts – Gestion des systèmes: Fonction de piste de vérification de sécurité.*
- Recommandation UIT-T X.741[3)] | ISO/CEI 10164-9...[3)], *Technologie de l'information – Interconnexion de systèmes ouverts – Gestion des systèmes: Objets et attributs pour le contrôle d'accès.*
- Recommandation UIT-T X.830[3)] | ISO/CEI 11586-1...[3)], *Technologies de l'information – Interconnexion des systèmes ouverts – Sécurité générique des couches supérieures: Vue d'ensemble, modèles et notation.*
- Recommandation UIT-T X.831[3)] | ISO/CEI 11586-2...[3)], *Technologies de l'information – Interconnexion des systèmes ouverts – Sécurité générique des couches supérieures: Définition du service assuré par l'élément de service d'échanges pour la sécurité.*
- Recommandation UIT-T X.832[3)] | ISO/CEI 11586-3...[3)], *Technologies de l'information – Interconnexion des systèmes ouverts – Sécurité générique des couches supérieures: Spécification des protocoles de l'élément de service d'échanges pour la sécurité.*
- Recommandation UIT-T X.833[3)] | ISO/CEI 11586-4...[3)], *Technologies de l'information – Interconnexion des systèmes ouverts – Sécurité générique des couches supérieures: Spécification de la syntaxe de protection du transfert.*

3) Actuellement à l'état de projet.