NORME INTERNATIONALE

ISO/CEI 10745

Première édition
1995-08-15

Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — Modèle de sécurité pour les couches supérieures

Information technology — Open Systems Interconnection — Upper layers security model

Numéro de référence
ISO/CEI 10745:1995(F)

Sommaire

Version française tirée en 1996

Imprimé en Suisse

Avant-propos

L'ISO (Organisation internationale de normalisation) et la CEI (Commission électrotechnique internationale) forment ensemble un système consacré à la normalisation internationale considérée comme un tout. Les organismes nationaux membres de l'ISO ou de la CEI participent au développement de Normes internationales par l'intermédiaire des comités techniques créés par l'organisation concernée afin de s'occuper des différents domaines particuliers de l'activité technique. Les comités techniques de l'ISO et de la CEI collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales ou non gouvernementales, en liaison avec l'ISO et la CEI participent également aux travaux.

Dans le domaine des technologies de l'information, l'ISO et la CEI ont créé un comité technique mixte, l'ISO/CEI JTC 1. Les projets de Normes internationales adoptés par le comité technique mixte sont soumis aux organismes nationaux pour approbation, avant leur acceptation comme Normes internationales. Les Normes internationales sont approuvées conformément aux procédures qui requièrent l'approbation de 75 % au moins des organismes nationaux votants.

La Norme internationale ISO/CEI 10745 a été élaborée par le comité technique mixte ISO/CEI JTC 1, *Technologies de l'information*, sous-comité SC 21, *Interconnexion des systèmes ouverts, gestion des données et traitement distribué ouvert*, en collaboration avec l'UIT-T. Le texte identique est publié en tant que Recommandation UIT-T X.803.

Les annexes A et B de la présente Norme internationale sont données uniquement à titre d'information.

Introduction

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 DE SYSTÈMES OUVERTS (OSI) — 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 9545:1994, *Technologies de l'information – Interconnexion de systèmes ouverts – Structure de la couche application.*
- Recommandation UIT-T X.811[1] (1993) | ISO/CEI 10181-2...[1], *Technologies de l'information – Interconnexion de systèmes ouverts – Cadres de sécurité pour systèmes ouverts – Cadre d'authentification.*
- Recommandation UIT-T X.812[1] (1993) | ISO/CEI 10181-3...[1], *Technologies de l'information – Interconnexion de systèmes ouverts – Cadres de sécurité pour 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 de 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 8822:1988, *Systèmes de traitement de l'information – Interconnexion de 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 8649:1988, *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 7498-2:1989, *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 I 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 I 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).