NORME INTERNATIONALE

ISO/CEI 10164-9

Première édition
1995-12-15

Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — Gestion-systèmes: Objets et attributs de contrôle d'accès

Information technology — Open Systems Interconnection — Systems Management: Objects and attributes for access control

Numéro de référence
ISO/CEI 10164-9:1995(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 vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des organismes nationaux votants.

La Norme internationale ISO/CEI 10164-9 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.741.

L'ISO/CEI 10164 comprend les parties suivantes, présentées sous le titre général *Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — Gestion-systèmes*:

— *Partie 1: Fonction de gestion d'objets*

— *Partie 2: Fonction de gestion d'états*

— *Partie 3: Attributs pour la représentation des relations*

— *Partie 4: Fonction de compte rendu d'alarme*

— *Partie 5: Fonction de gestion de rapport événementiel*

— *Partie 6: Fonction de contrôle de journal*

— *Partie 7: Fonction de compte rendu d'alarme de sécurité*

— *Partie 8: Fonction de sécurité de l'expertise de l'historique*

— *Partie 9: Objets et attributs de contrôle d'accès*

— *Partie 10: Fonction de comptage d'utilisation aux fins de comptabilité*

— *Partie 11: Objets et attributs métriques*

— *Partie 12: Fonction de gestion des tests*

— *Partie 13: Fonction de récapitulation*

— *Partie 14: Catégories de test de confiance et de diagnostic*

— *Partie 15: Fonction de programmation*

— *Partie 16: Fonction de gestion pour la gestion de connaissance*

— *Partie 17: Fonction de changement*

— *Partie 18: Fonction de gestion de logiciel*

— *Partie 19: Fonctions de gestion de police de gestion et de domaine de gestion*

Les annexes A à F font partie intégrante de la présente partie de l'ISO/CEI 10164. Les annexes G et H sont données uniquement à titre d'information.

Introduction

La présente Recommandation I Norme internationale spécifie un modèle de sécurité pour le contrôle d'accès ainsi que les informations de gestion qui sont nécessaires afin de créer et d'administrer le contrôle d'accès associé à la gestion des systèmes OSI. La politique de sécurité adoptée dans chaque instance d'utilisation n'est pas spécifiée et est laissée aux soins des réalisateurs. La présente Spécification est générique et applicable à la gestion de la sécurité de nombreux types d'application. Il est prévu qu'elle soit utilisée par les réseaux RGT.

NORME INTERNATIONALE

RECOMMANDATION UIT-T

TECHNOLOGIES DE L'INFORMATION – INTERCONNEXION DE SYSTÈMES OUVERTS (OSI) – GESTION-SYSTÈMES: OBJETS ET ATTRIBUTS DE CONTRÔLE D'ACCÈS

1 Domaine d'application

Les spécifications contenues dans les articles ci-dessous sont applicables à la fourniture du contrôle d'accès dans les applications utilisant les services et protocoles de gestion OSI.

La présente Recommandation | Norme internationale:

- établit les besoins de l'utilisateur pour la fourniture du service de contrôle d'accès dans les applications utilisant les services et protocoles de gestion OSI;
- interprète et applique le modèle général de contrôle d'accès qui est défini dans la Rec. UIT-T X.812 | ISO/CEI 10181-3 et qui doit être utilisé dans les applications de gestion faisant appel aux services et protocoles de gestion OSI;
- définit des procédures pour l'application de règles de contrôle d'accès en liaison avec l'utilisation des services et protocoles de gestion OSI;
- définit des classes d'objets gérés et des types d'attribut:
  a) qui représentent certaines des informations de contrôle d'accès pouvant être utilisées pour fournir le service de contrôle d'accès; et
  b) qui ne peuvent être utilisés que lorsque la gestion des informations de contrôle d'accès doit être réalisée par la gestion des systèmes;
- spécifie le protocole nécessaire à l'échange des informations de contrôle d'accès définies dans la présente Recommandation | Norme internationale, lorsque l'échange est réalisé selon la gestion des systèmes OSI;
- spécifie les prescriptions de conformité pour les systèmes ouverts revendiquant la compatibilité avec le service de contrôle d'accès pour les applications faisant appel aux services et protocoles de gestion OSI;
- spécifie les prescriptions de conformité pour les systèmes ouverts revendiquant la compatibilité avec le service de contrôle d'accès défini dans la présente Recommandation | Norme internationale.

Les informations de contrôle d'accès figurant dans la présente Recommandation | Norme internationale pourront être utilisées pour mettre en œuvre des modes de contrôle d'accès fondés sur des listes de contrôle d'accès, sur des capacités, sur des étiquettes de sécurité et sur des contraintes contextuelles.

La présente Recommandation | Norme internationale:

- ne définit pas de politique de contrôle d'accès pour les applications qui font appel aux services et protocoles de gestion OSI;
- ne définit pas les domaines de sécurité (ou de gestion) dans lesquels une politique de contrôle d'accès peut être imposée;
- ne définit pas la manière dont les composantes d'une fonction de contrôle d'accès seront mises en œuvre ni à quel endroit ces composantes devront se trouver;
- ne spécifie pas la forme d'une quelconque information de contrôle d'accès qui est enregistrée à titre temporaire ou permanent dans un système ouvert;
- ne spécifie ni ne prescrit aucun mécanisme de contrôle d'accès particulier;
- ne prescrit pas de gérer les informations de contrôle d'accès ni, si elles doivent l'être, qu'elles le soient au moyen de la gestion des systèmes OSI;

- ne décrit pas la manière dont les entités d'application de gestion agissent, en cours de communication, pour prendre des décisions de contrôle d'accès au nom ou pour le compte d'une tierce partie quelconque;
- ne spécifie aucune exigence de conformité pour le paramètre de contrôle d'accès défini dans la présente Recommandation I Norme internationale.

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 I Norme internationale. Au moment de la publication, les éditions indiquées étaient en vigueur. Toute Recommandation ou Norme est sujette à révision et les parties prenantes aux accords fondés sur la présente Recommandation I Norme internationale sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et Normes 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 tient à jour une liste des Recommandations UIT-T en vigueur.

2.1 Recommandations I Normes internationales identiques

- Recommandation UIT-T X.200 (1994) I ISO/CEI 7498-1:1994, *Technologie de l'information – Interconnexion de systèmes ouverts – Modèle de référence de base: Le modèle de référence de base.*
- Recommandation UIT-T X.509 (1993) I ISO/CEI 9594-8:1995, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: Cadre d'authentification.*
- Recommandation X.701 du CCITT (1992)[1] I ISO/CEI 10400:1992[1], *Technologies de l'information – Interconnexion des systèmes ouverts – Aperçu général de la gestion des systèmes.*
- Recommandation X.720 du CCITT (1992) I ISO/CEI 10165-1:1993, *Technologie de l'information – Interconnexion des systèmes ouverts – Structure des informations de gestion: Modèle d'information de gestion.*
- Recommandation X.721 du CCITT (1992) I ISO/CEI 10165-2:1992, *Technologie de l'information – Interconnexion des systèmes ouverts – Structure des informations de gestion: Définition des informations de gestion.*
- Recommandation X.722 du CCITT (1992) I ISO/CEI 10165-4:1992, *Technologie de l'information – Interconnexion des systèmes ouverts – Structure des informations de gestion: Directives pour la définition des objets gérés.*
- Recommandation UIT-T X.724 (1993) I ISO/CEI 10165-6:1994, *Technologie de l'information – Interconnexion des systèmes ouverts – Structure de l'information de gestion: Spécifications et directives pour l'établissement des formulaires de déclaration de conformité d'instances associés à la gestion OSI.*
- Recommandation X.730 du CCITT (1992) I ISO/CEI 10164-1:1993, *Technologie de l'information – Interconnexion des systèmes ouverts – Gestion des systèmes: Fonction de gestion des objets.*
- Recommandation X.731 du CCITT (1992) I ISO/CEI 10164-2:1993, *Technologie de l'information – Interconnexion des systèmes ouverts – Gestion des systèmes: Fonction de gestion d'états.*
- Recommandation X.732 du CCITT (1992) I ISO/CEI 10164-3:1993, *Technologie de l'information – Interconnexion des systèmes ouverts – Gestion des systèmes: Attributs relationnels.*
- Recommandation X.734 du CCITT (1992) I ISO/CEI 10164-5:1993, *Technologie de l'information – Interconnexion des systèmes ouverts – Gestion des systèmes: Fonction de gestion des rapports d'événement.*
- Recommandation X.736 du CCITT (1992) I ISO/CEI 10164-7:1992, *Technologie de l'information – Interconnexion des systèmes ouverts – Gestion des systèmes: Fonction de signalisation des alarmes de sécurité.*
- Recommandation X.740 du CCITT (1992) I ISO/CEI 10164-8:1993, *Technologie de l'information – Interconnexion des systèmes ouverts – Gestion des systèmes: Fonction de piste de vérification de sécurité.*

[1] Modifiée par Rec. UIT-T X.701/Cor.2 I ISO/CEI 10040/Cor.2.

- Recommandation UIT-T X.810[2] | ISO/CEI 10181-1 ...[2], *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité dans les systèmes ouverts: Vue d'ensemble.*
- Recommandation UIT-T X.812[2] | ISO/CEI 10181-3 ...[2], *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité dans les systèmes ouverts: Contrôle d'accès.*

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

- Recommandation X.208 du CCITT (1988), *Spécification de la syntaxe abstraite numéro un (ASN.1).*

  ISO/CEI 8824:1990, *Technologies de l'information – Interconnexion de systèmes ouverts – Spécification de la notation de syntaxe abstraite numéro un (ASN.1).*
- Recommandation X.209 du CCITT (1988), *Spécification des règles de codage de base pour la notation de syntaxe abstraite numéro un (ASN.1).*

  ISO/CEI 8825:1990, *Technologies de l'information – Interconnexion de systèmes ouverts – Spécification de règles de base pour coder la notation de la syntaxe abstraite numéro un (ASN.1).*
- Recommandation X.217 du CCITT (1992), *Technologies de l'information – Interconnexion des systèmes ouverts – Définition du service applicable à l'élément de service de contrôle d'association.*

  ISO 8649:1988[3], *Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Définition du service pour l'élément de service de contrôle d'association.*
- Recommandation X.227 du CCITT (1992), *Technologies de l'information – Interconnexion des systèmes ouverts – Protocole en mode connexion applicable à l'élément de service de contrôle d'association: Spécification du protocole.*

  ISO 8650:1988[4], *Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Spécification du protocole pour l'élément de service de contrôle d'association.*
- Recommandation X.290 du CCITT (1992), *Cadre général et méthodologie des tests de conformité OSI pour les Recommandations sur les protocoles pour les applications du CCITT – Concepts généraux.*

  ISO/CEI 9646-1:1994, *Technologies de l'information – Interconnexion de systèmes ouverts – Cadre général et méthodologie des tests de conformité – Partie 1: Concepts généraux.*
- Recommandation X.291 du CCITT (1992), *Cadre général et méthodologie des tests de conformité OSI pour les Recommandations sur les protocoles pour les applications du CCITT – Spécification de suite de tests abstraite.*

  ISO/CEI 9646-2:1994, *Technologies de l'information – Interconnexion de systèmes ouverts – Cadre général et méthodologie des tests de conformité OSI – Partie 2: Spécification des suites de tests abstraites.*
- Recommandation UIT-T X.296[2], *Cadre général et méthodologie des tests de conformité OSI pour les Recommandations sur les protocoles pour les applications de l'UIT-T – Déclarations de conformité d'instance.*

  ISO/CEI 9646-7:1995, *Technologies de l'information – Interconnexion des systèmes ouverts – Cadre général et méthodologie des tests de conformité OSI – Partie 7: Implementation conformance statements.*
- 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.710 du CCITT (1991), *Définition du service commun de transfert d'informations de gestion pour les applications du CCITT.*

  ISO/CEI 9595:1991, *Technologies de l'information – Interconnexion de systèmes ouverts – Définition du service commun d'informations de gestion.*
- Recommandation X.711 du CCITT (1991), *Spécification du protocole commun de transfert d'informations de gestion pour les applications du CCITT.*

---

2) Actuellement à l'état de projet.

3) Modifiée par ISO/CEI 8649:1988/Amd.1:1990.

4) Modifiée par ISO/CEI 8650:1988/Amd.1:1990.

ISO/CEI 9596-1:1991, *Technologies de l'information – Interconnexion de systèmes ouverts – Protocole commun d'information de gestion – Partie 1: Spécification.*

– 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

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

3.1 Définitions relatives au modèle de référence

La présente Recommandation | Norme internationale utilise le terme suivant, qui est défini dans la Rec. UIT-T X.200 | ISO/CEI 7498-1:

– système ouvert.

3.2 Définitions relatives à l'architecture de sécurité

La présente Recommandation | Norme internationale utilise les termes suivants, qui sont définis dans la Rec. X.800 du CCITT | ISO 7498-2:

a) contrôle d'accès;

b) liste de contrôle d'accès;

c) authentification;

d) capacité;

e) étiquette de sécurité;

f) politique de sécurité.

3.3 Définitions relatives au cadre de gestion

La présente Recommandation | Norme internationale utilise les termes suivants, qui sont définis dans la Rec. X.700 du CCITT | ISO/CEI 7498-4:

a) objet géré;

b) entité d'application de gestion des systèmes.

3.4 Définitions relatives à la vue d'ensemble des cadres de sécurité

La présente Recommandation | Norme internationale utilise les termes suivants, qui sont définis dans la Rec. UIT-T X.810 | ISO/CEI 10181-1:

a) certificat de sécurité;

b) domaine de sécurité;

c) jeton de sécurité.

3.5 Définitions relatives au cadre de contrôle d'accès

La présente Recommandation | Norme internationale utilise les termes suivants, qui sont définis dans la Rec. UIT-T X.812 | ISO/CEI 10181-3:

a) certificat de contrôle d'accès;

b) information décisionnelle de contrôle d'accès (ADI);

c) fonction décisionnelle de contrôle d'accès (ADF);

d) fonction exécutive de contrôle d'accès (AEF);

e) information de contrôle d'accès (ACI);

f) politique de contrôle d'accès;

g) information contextuelle;

h) initiateur;

i) information décisionnelle de contrôle d'accès issue de l'initiateur (information ADI d'initiateur);

j) information de contrôle d'accès issue de l'initiateur (information ACI d'initiateur);

k) information de contrôle d'accès liée à l'initiateur (information ACI liée à l'initiateur);

l) information décisionnelle de contrôle d'accès issue de l'opérande (information ADI d'opérande);

m) information de contrôle d'accès liée à l'opérande (information ACI liée à l'opérande);

n) information ADI retenue;

o) cible;

p) information décisionnelle de contrôle d'accès issue de la cible (information ADI de cible);

q) information de contrôle d'accès issue de la cible (information ACI de cible);

r) information de contrôle d'accès liée à la cible (information ACI liée à la cible).

3.6 Définitions relatives à la vue d'ensemble de la gestion des systèmes

La présente Recommandation | Norme internationale utilise les termes suivants, qui sont définis dans la Rec. X.701 du CCITT | ISO/CEI 10040:

a) définitions génériques;

b) classe d'objets gérés;

c) formulaire de déclaration de conformité d'objet de gestion (MOCS);

d) formulaire de déclaration de conformité d'information de gestion (MICS);

e) opération de gestion;

f) formulaire MICS;

g) formulaire MOCS;

h) notification.

3.7 Définitions relatives au modèle d'informations de gestion

La présente Recommandation | Norme internationale utilise les termes suivants, qui sont définis dans la Rec. X.720 du CCITT | ISO/CEI 10165-1:

a) action;

b) caractéristique.

3.8 Définitions relatives au formulaire de déclaration de conformité d'instance

La présente Recommandation | Norme internationale utilise les termes suivants, qui sont définis dans la Rec. UIT-T X.724 | ISO/CEI 10165-6:

a) déclaration de conformité de relation gérée (MRCS);

b) récapitulatif de conformité de gestion (MCS);

c) formulaire de déclaration de définition d'information de gestion (MIDS);

d) formulaire MCS;

e) formulaire MRCS.

3.9 Définitions relatives à la gestion des rapports d'événement

La présente Recommandation | Norme internationale utilise le terme suivant, qui est défini dans la Rec. X.734 du CCITT | ISO/CEI 10164-5:

– discriminateur de retransmission (de rapport) d'événement.

3.10 Définitions relatives aux tests de conformité OSI

La présente Recommandation I Norme internationale utilise les termes suivants, qui sont définis dans la Rec. X.290 du CCITT I ISO/CEI 9646-1:

a) formulaire PICS;

b) déclaration de conformité d'instance de protocole;

c) déclaration de conformité d'un système.

3.11 Autres définitions

3.11.1 **autorité domaniale de sécurité**: Entité chargée de la mise en œuvre d'une politique de sécurité.

3.11.2 **type d'opération**: Action effectuée sur un objet géré à la suite d'une demande de gestion.

4 Symboles et abréviations

ACC Certificat de contrôle d'accès (*access control certificate*)

ADI Information décisionnelle de contrôle d'accès (*access control decision information*)

ACI Information de contrôle d'accès (*access control information*)

ACL Liste de contrôle d'accès (*access control list*)

ADF Fonction décisionnelle de contrôle d'accès (*access control decision function*)

AEF Fonction exécutive de contrôle d'accès (*access control enforcement function*)

CMIS Service commun d'information de gestion (*common management information service*)

CMIP Protocole commun d'information de gestion (*common management information protocol*)

ICS Déclaration de conformité d'instance (*implementation conformance statement*)

MAPDU Unité de données du protocole d'application de gestion (*management application protocol data unit*)

MCS Récapitulatif de conformité de gestion (*management conformance summary*)

MICS Déclaration de conformité d'information de gestion (*management information conformance statement*)

MIDS Déclaration de définition d'information de gestion (*management information definition statement*)

MOCS Déclaration de conformité d'objet de gestion (*managed object conformance statement*)

MRCS Déclaration de conformité de relation gérée (*managed relationship conformance statement*)

PAC Certificat d'accès privilégié (*privilege attribute certificate*)

PICS Déclaration de conformité d'instance de protocole (*protocol implementation conformance statement*)

SMAE Entité d'application de gestion des systèmes (*systems management application entity*)

5 Conventions

La présente Recommandation I Norme internationale fait appel aux techniques de notation spécifiées dans la Rec. X.722 du CCITT I ISO/CEI 10165-4 pour la définition des objets gérés et de leurs attributs.

6 Prescriptions

Un utilisateur des services de gestion OSI a besoin qu'un mécanisme de contrôle d'accès, unique ou multiple, empêche tout accès non autorisé aux applications de gestion et aux informations de gestion.

Le contrôle d'accès aux informations de gestion est requis dans chacun des trois cas suivants:

a) pour protéger les informations de gestion d'une création, suppression, modification ou divulgation non autorisée, due à une opération de gestion OSI;

b) pour faire en sorte que seuls les initiateurs soient en mesure d'utiliser les opérations de gestion pour lesquelles des droits d'accès ont été accordés au cours de l'établissement de l'association d'application; et

c) pour empêcher l'envoi d'informations de gestion à des destinataires non autorisés, en raison de rapports d'événement de type confirmé ou non confirmé.

NOTE – Pour être complet, il faut ajouter la nécessité du contrôle d'accès à des associations. Ce sujet fera l'objet d'une étude complémentaire.

Divers niveaux de contrôle d'accès peuvent être requis. Par exemple, certains utilisateurs peuvent recevoir un accès en lecture et en écriture à des attributs spécifiques, alors que d'autres ne peuvent avoir qu'un accès en lecture ou aucun accès. Certains utilisateurs peuvent ne se voir accorder des droits d'accès qu'à certains objets de gestion spécifiques alors que d'autres utilisateurs peuvent accéder à un ensemble différent d'objets de gestion. Pour les opérations de gestion, des restrictions d'accès sont nécessaires pour protéger des objets gérés, des attributs particuliers d'objets gérés, des valeurs d'attributs particuliers, un contexte d'accès ou des actions associées à l'objet géré.

Il est prescrit de prévoir un paramètre de contrôle d'accès pouvant être utilisé dans les échanges d'informations de gestion au moyen du service CMIS.

Il est également prescrit que les systèmes ouverts assurant le contrôle d'accès à des applications de gestion OSI, ainsi que les protocoles à observer, manifestent le même comportement en termes de contrôle d'accès lors de l'application du même ensemble de règles de contrôle d'accès.

Il est prescrit que les dispositions de la présente Recommandation | Norme internationale n'empêchent pas l'utilisation de mécanismes de contrôle d'accès non identifiés dans son cadre.

De manière à réaliser la gestion des informations de contrôle d'accès au moyen de la gestion des systèmes OSI, il est nécessaire:

- que ces informations soient modélisées sous la forme d'objets gérés de façon qu'elles puissent être créées, supprimées, modifiées et lues;
- que l'on puisse déterminer les cibles auxquelles un initiateur peut avoir accès;
- et que l'on puisse déterminer les initiateurs qui peuvent avoir accès à une cible donnée.

Il est prescrit que l'on puisse empêcher la découverte – au moyen d'un analyseur-lecteur de signal – des objets gérés qui sont contenus dans un sous-arbre d'informations de gestion.

Il est prescrit que l'on puisse empêcher l'application générale d'une opération (comme une suppression) au moyen d'un analyseur-conditionneur de signal.

Il est prescrit que l'on puisse attribuer des étiquettes de sécurité uniques à des cibles spécifiques.

7 Interprétation du modèle de contrôle d'accès

7.1 Vue d'ensemble du modèle de contrôle d'accès

Le contrôle d'accès pour la gestion OSI est fondé sur le modèle défini à cette fin dans la Rec. UIT-T X.812 | ISO/CEI 10181-3. Dans ce modèle de base, les fonctions de décision et d'exécution du contrôle d'accès sont interposées entre l'initiateur et la cible. La présente Recommandation | Norme internationale montre comment ce modèle s'applique à la fourniture du contrôle d'accès à des applications utilisant les services et protocoles de gestion OSI.

La fonction décisionnelle de contrôle d'accès nécessite des informations placées sous l'appellation générique d'informations de contrôle d'accès (ACI), utilisées dans le processus de prise de décision. Les informations de contrôle d'accès peuvent être modélisées sous la forme d'informations de gestion et peuvent être décrites au moyen des techniques de notation spécifiées dans la Rec. X.722 du CCITT | ISO/CEI 10165-4. La présente Recommandation | Norme internationale définit certaines informations de contrôle d'accès sous la forme d'attributs de classes d'objets gérés, de manière que la gestion des systèmes OSI puisse servir à échanger ces informations entre des systèmes ouverts.

NOTE – La présente Recommandation | Norme internationale ne spécifie pas la forme ou la structure réelle d'une information de contrôle d'accès qui est stockée temporairement ou durablement dans un système ouvert. En revanche, elle spécifie la syntaxe abstraite des éléments d'information ACI qui peuvent être échangés par des systèmes ouverts au moyen de la gestion des systèmes OSI.

Tous les modes de contrôle d'accès identifiés dans la Rec. UIT-T X.812 | ISO/CEI 10181-3 – modes par liste ACL, par capacité, par contexte et par étiquette – sont applicables à la fourniture du service de contrôle d'accès aux applications utilisant les services et protocoles de gestion OSI. Ces modes de contrôle d'accès peuvent être utilisés isolément ou en combinaison, de manière que le contrôle d'accès puisse être assuré conformément à une politique de contrôle d'accès appropriée au domaine de sécurité.

Le contrôle d'accès est régi par une politique de contrôle d'accès. Lorsqu'une politique spécifique de contrôle d'accès est appliquée à un groupe d'éléments, la combinaison de ces derniers et de cette politique de contrôle d'accès délimite un domaine de sécurité spécifique. Une seule politique de contrôle d'accès est exécutée à un moment donné dans un domaine de sécurité donné.

L'authentification de l'utilisateur de la gestion OSI et l'authentification symétrique des entités SMAE sont hors du domaine d'application de la présente Recommandation | Norme internationale. Les procédures de contrôle d'accès qui y sont définies exigent toutefois l'emploi de procédures d'authentification au moment approprié. La Rec. X.217 du CCITT | ISO 8649, la Rec. X.227 du CCITT | ISO 8650 et la Rec. UIT-T X.509 | ISO/CEI 9594-8 décrivent des procédures d'authentification possibles.

Le contrôle d'accès pour la gestion OSI est spécifié sous la forme d'un ensemble de refus et d'autorisations d'exécuter des opérations de gestion. L'utilisateur de l'application de gestion qui invoque l'opération de gestion est l'initiateur et les éléments d'information de gestion identifiés par les paramètres de l'opération de gestion, par exemple des objets gérés et des attributs, se combinent pour former la cible (ou les cibles).

Le contrôle d'accès des rapports d'événement s'effectue par application des procédures de contrôle d'accès aux opérations de gestion se rapportant aux discriminateurs de retransmission de rapport d'événement.

7.2 Politiques de contrôle d'accès

Une politique de contrôle d'accès comporte un ou plusieurs ensembles de règles. Il appartient au maître d'œuvre de la politique de contrôle d'accès de veiller à ce que les règles de contrôle d'accès donnent une image fidèle de l'instanciation de la politique de contrôle d'accès.

Une politique de contrôle d'accès est une politique de gestion spécifique qui peut être soumise à une administration de politique de gestion.

NOTE – La présente Recommandation | Norme internationale ne spécifie pas la gestion des politiques de gestion et, en particulier, ne spécifie aucun moyen de vérification de l'intégrité des informations de contrôle d'accès.

Une politique de contrôle d'accès est exécutée au moyen d'un ou de plusieurs des modes de contrôle d'accès suivants:

- modes par liste ACL;
- modes par capacités;
- modes par contexte; et
- modes par étiquette.

Si certaines caractéristiques d'un objet géré (par exemple ses attributs) sont placées sous la dépendance de différentes politiques de sécurité, cet objet géré peut appartenir à plusieurs domaines de sécurité. Lorsque plusieurs politiques de contrôle d'accès s'appliquent à un même objet géré, la politique de contrôle d'accès à exécuter est celle qui est associée à la fois à l'initiateur et à la cible.

7.3 Informations de contrôle d'accès

Les informations de contrôle d'accès (ACI) comprennent:

- les règles de contrôle d'accès;
- l'identité de l'initiateur de la demande d'accès (information ACI d'initiateur);
- les capacités et habilitations de sécurité associées à l'initiateur (information ACI d'initiateur);
- les informations relatives à l'authentification de l'initiateur (information ADI d'initiateur);
- les identités d'information de gestion (cibles) auxquelles l'accès a été demandé (information ACI de cible);
- les capacités et habilitations de sécurité associées à la cible (information ACI de cible);
- les opérations autorisées qui peuvent être exécutées sur les informations de gestion (information ACI d'initiateur, information ACI de cible);
- les informations retenues par la fonction décisionnelle de contrôle d'accès pour usage ultérieur (informations ADI retenues); et
- les informations contextuelles.

7.3.1 règles de contrôle d'accès: Informations de contrôle d'accès qui représentent les opérations permises et les conditions de leur exécution dans un domaine de sécurité donné. Il y a cinq classes de règles de contrôle d'accès, qui doivent être appliquées par la fonction ADF:

- **règles de refus globales** – Règles de contrôle d'accès qui refusent l'accès à toutes les cibles. Si une règle globale refuse l'accès, aucune autre règle ne doit s'appliquer. Si une règle globale ne refuse pas l'accès, les règles de refus d'item sont appliquées;
- **règles de refus d'item** – Règles de contrôle d'accès qui refusent l'accès à certaines cibles. Si une règle d'item refuse l'accès, aucune autre règle ne doit s'appliquer. Si une règle d'item ne refuse pas l'accès, les règles de refus globales sont appliquées;
- **règles d'autorisation globales** – Règles de contrôle d'accès qui autorisent l'accès à toutes les cibles. Si une règle globale autorise l'accès, aucune autre règle ne doit s'appliquer. Si une règle globale n'autorise pas l'accès, les règles d'autorisation d'item sont appliquées;
- **règles d'autorisation d'item** – Règles de contrôle d'accès qui autorisent l'accès à certaines cibles. Si une règle d'autorisation autorise l'accès, aucune autre règle ne doit s'appliquer. Si une règle d'item n'autorise pas l'accès, les règles par défaut sont appliquées;
- **règles par défaut** – Règles de contrôle d'accès qui doivent être appliquées lorsque aucune autre règle n'a expressément autorisé ou refusé l'accès. Les règles par défaut doivent autoriser ou refuser l'accès.

7.3.2 information ACI liée à l'action: Information de contrôle d'accès (par exemple une étiquette de sécurité) qui est associée à l'information de gestion acheminée dans les opérations de gestion et dans les rapports d'événement. Les informations ACI liées à l'action peuvent également servir à créer et/ou à modifier des informations de contrôle d'accès associées à une cible.

7.3.3 information ACI liée à l'initiateur: Information de contrôle d'accès fournie par une demande de gestion issue de l'initiateur ou associée d'une autre façon à une telle demande. Ces informations peuvent prendre l'une des formes suivantes:

- identité de l'initiateur de l'opération de gestion;
- information insérée dans le paramètre contrôle d'accès d'opérations de gestion (par exemple le paramètre de contrôle d'accès dans le service CMIS ou le paramètre de contrôle d'accès aux informations d'utilisateur dans le protocole CMIP);

- information désignée par une autorité de domaine de sécurité; ou
- une combinaison des informations ci-dessus.

Le paramètre de contrôle d'accès acheminé par le service CMIS peut prendre la forme d'un certificat de sécurité ou d'un jeton de sécurité.

NOTE – L'identité de l'initiateur peut être communiquée par des mécanismes d'authentification au moyen de procédures locales qui sont hors du domaine d'application de la présente Recommandation | Norme internationale.

7.3.4 information ACI liée à la cible: Information de contrôle d'accès qui désigne l'information de gestion sur laquelle des opérations doivent être exécutées.

7.3.5 information contextuelle: Information de contrôle d'accès associée au contexte (par exemple l'heure du jour, le niveau d'authentification, le lieu, les ressources disponibles, la participation à une relation).

7.3.6 information ADI: Information décisionnelle de contrôle d'accès pour une action, pour un initiateur ou pour une cible, déduite de l'information ACI liée à l'action, à l'initiateur ou à la cible selon le cas, en vue de la prise d'une décision.

7.3.7 information ADI retenue: Information de contrôle d'accès qui est retenue par la fonction décisionnelle de contrôle d'accès. Conformément à la politique de contrôle d'accès, une partie de cette information peut être retenue pendant des périodes plus longues que la durée de vie d'une association. Les informations ADI retenues peuvent être utilisées par la fonction ADF pour évaluer des privilèges d'accès.

7.4 Procédures de contrôle d'accès

Les règles de contrôle d'accès spécifient les critères de sécurité qui doivent être satisfaits pour que l'on autorise l'accès à des informations de gestion. Ces règles peuvent prescrire l'exécution d'une partie ou de la totalité des procédures suivantes:

- validation des informations ACI liées à l'initiateur;
- identification de la cible;