NORME INTERNATIONALE

ISO/CEI 10181-3

Première édition
1996-09-15

Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — Cadres de sécurité pour les systèmes ouverts: Cadre de contrôle d'accès

Information technology — Open Systems Interconnection — Security frameworks for open systems: Access control framework

Numéro de référence
ISO/CEI 10181-3:1996(F)

Sommaire

Version française tirée en 1997

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 10181-3 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.812.

L'ISO/CEI 10181 comprend les parties suivantes, présentées sous le titre général *Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — Cadres de sécurité pour les systèmes ouverts*:

— *Partie 1: Présentation*

— *Partie 2: Cadre d'authentification*

— *Partie 3: Cadre de contrôle d'accès*

— *Partie 4: Cadre de non-répudiation*

— *Partie 5: Cadre de confidentialité*

— *Partie 6: Cadre d'intégrité*

— *Partie 7: Cadre d'audit de sécurité*

Les annexes A à G de la présente partie de l'ISO/CEI 10181 sont données uniquement à titre d'information.

Introduction

La présente Recommandation | Norme internationale définit un cadre général pour la fourniture du contrôle d'accès. Le but essentiel du contrôle d'accès est de parer au risque d'opérations non autorisées au moyen d'un ordinateur ou d'un système de communication; ces menaces sont fréquemment subdivisées en classes qui sont notamment les suivantes: utilisation non autorisée, divulgation, modification, destruction ou déni de service.

NORME INTERNATIONALE

RECOMMANDATION UIT-T

TECHNOLOGIES DE L'INFORMATION – INTERCONNEXION DE SYSTÈMES OUVERTS (OSI) – CADRES DE SÉCURITÉ POUR LES SYSTÈMES OUVERTS: CADRE DE CONTRÔLE D'ACCÈS

1 Domaine d'application

Les cadres de sécurité sont destinés à traiter l'application des services de sécurité dans l'environnement des systèmes ouverts, où le terme *systèmes ouverts* est utilisé pour des domaines tels que les bases de données, les applications distribuées, le traitement ODP et l'interconnexion OSI. Les cadres de sécurité sont destinés à définir les moyens d'offrir la protection des systèmes et des objets au sein des systèmes, ainsi que les interactions entre systèmes. Les cadres ne traitent pas de la méthodologie de construction des systèmes ou des mécanismes.

Les cadres couvrent à la fois les éléments de données et les séquences d'opérations (mais pas les éléments de protocole) utilisés pour obtenir des services spécifiques de sécurité. Ces services de sécurité peuvent s'appliquer aux entités communicantes des systèmes aussi bien qu'aux données échangées entre systèmes, et aux données gérées par les systèmes.

Dans le cas du contrôle d'accès, les accès peuvent être destinés *à* un système (par exemple, vers une entité qui est la partie communicante d'un système) ou prendre place *au sein* d'un système. Les éléments de données qui doivent être présentés pour obtenir l'accès, ainsi que la séquence d'opérations de la demande et pour la notification des résultats de l'accès, sont considérés comme faisant partie des cadres de sécurité. Cependant, tout élément de données et toute opération qui dépend seulement d'une application et qui est strictement concerné par l'accès local au sein d'un système ne fait pas partie du domaine d'application des cadres de sécurité.

Plusieurs applications ont des besoins de sécurité pour protéger des menaces sur des ressources, y compris l'information, résultant de l'interconnexion des systèmes ouverts. Certaines menaces communément connues, dans un environnement OSI, ainsi que les services et mécanismes de sécurité pour s'en protéger, sont décrits dans la Rec. X.800 du CCITT | ISO 7498-2.

Le processus de détermination des utilisations de ressources permises dans un environnement de système ouvert et, lorsque cela est approprié, la prévention contre un accès non autorisé est appelé contrôle d'accès. La présente Recommandation | Norme internationale définit un cadre général pour la fourniture des services de contrôle d'accès.

Ce cadre de sécurité:

a) définit les concepts élémentaires du contrôle d'accès;

b) démontre la façon dont les concepts élémentaires du contrôle d'accès peuvent être spécialisés pour mettre en œuvre quelques services et mécanismes d'accès communément reconnus;

c) définit ces services et mécanismes de contrôle d'accès correspondants;

d) identifie les besoins fonctionnels des protocoles pour la mise en œuvre de ces services et mécanismes de contrôle d'accès;

e) identifie les besoins de gestion afin de mettre en œuvre ces services et mécanismes de contrôle d'accès;

f) couvre l'interaction des services et mécanismes de contrôle d'accès avec d'autres services et mécanismes de sécurité.

Comme pour les autres services de sécurité, le contrôle d'accès peut être fourni seulement dans le contexte d'une politique de sécurité définie pour une application particulière. La définition des politiques de contrôle d'accès ne fait pas partie du domaine d'application de la présente Recommandation | Norme internationale, cependant, certaines caractéristiques des politiques de contrôle d'accès sont présentées.

L'objet de la présente Recommandation | Norme internationale n'est pas de spécifier les détails des échanges de protocoles qui peuvent s'avérer nécessaires pour fournir les services de contrôle d'accès.

La présente Recommandation | Norme internationale ne spécifie pas de mécanisme particulier pour mettre en œuvre ces services de contrôle d'accès ni les détails des services et protocoles de gestion de la sécurité.

Différents types de normes peuvent utiliser ce cadre y compris:

a) les normes qui incorporent le concept du contrôle d'accès;

b) les normes qui spécifient les services d'accès incluant le contrôle d'accès;

c) les normes qui spécifient les utilisations d'un service de contrôle d'accès;

d) les normes qui spécifient les moyens de fournir le contrôle d'accès au sein d'un environnement de système ouvert;

e) les normes qui spécifient les mécanismes de contrôle d'accès.

De telles normes peuvent utiliser ce cadre de la façon suivante:

– les normes de types a), b), c), d) et e) peuvent utiliser la terminologie de ce cadre;

– les normes de types b), c), d) et e) peuvent utiliser les fonctionnalités définies dans l'article 7 de ce cadre;

– la norme de type e) peut être fondée sur les classes de mécanismes définies dans l'article 8 de ce cadre.

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. Toutes Recommandations et Normes sont sujettes 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 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 de l'UIT-T en vigueur.

2.1 Recommandations | Normes internationales identiques

– Recommandation UIT-T X.200 (1994) | ISO/CEI 7498-1:1994, *Technologies de l'information – Interconnexion des systèmes ouverts – Modèle de référence de base: le modèle de référence de base.*

– Recommandation UIT-T X.810 (1995) | ISO/CEI 10181-1:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: aperçu général.*

– Recommandation UIT-T X.811 (1995) | ISO/CEI 10181-2:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Cadre de sécurité pour systèmes ouverts: cadre d'authentification.*

– Recommandation UIT-T X.880 (1994) | ISO/CEI 13712-1:1995, *Technologies de l'information – Opérations distantes: concepts, modèle et notation.*

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

– Recommandation X.800 du CCITT (1991), *Architecture de sécurité pour l'interconnexion des 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 La présente Recommandation | Norme internationale utilise les termes suivants définis dans la Rec. X.800 du CCITT | ISO 7498-2:

a) contrôle d'accès;

b) liste de contrôle d'accès;

c) imputabilité;

d) authentification;

e) information d'authentification;

f) autorisation;

g) capacité;

h) politique de sécurité fondée sur l'identité;

i) politique de sécurité fondée sur des règles;

j) audit de sécurité;

k) label de sécurité;

l) politique de sécurité;

m) service de sécurité;

n) sensibilité.

3.2 La présente Recommandation | Norme internationale utilise les termes suivants définis dans la Rec. UIT-T X.810 | ISO/CEI 11081-1:

a) politique d'interaction sécurisée;

b) certificat de sécurité;

c) domaine de sécurité;

d) autorité du domaine de sécurité;

e) information de sécurité;

f) règles de politique de sécurité;

g) jeton de sécurité;

h) confiance.

3.3 La présente Recommandation | Norme internationale utilise les termes suivants définis dans la Rec. UIT-T X.200 | ISO/CEI 7498-1:

– système réel.

3.4 Les définitions suivantes s'appliquent pour la présente Recommandation | Norme internationale:

3.4.1 certificat de contrôle d'accès: Certificat de sécurité contenant l'information ACI.

3.4.2 information de décision de contrôle d'accès (ADI) (*access control decision information*): Partie (éventuellement toute) de l'information ACI fournie à la fonction ADF pour décider d'un contrôle d'accès particulier.

3.4.3 fonction de décision de contrôle d'accès (ADF) (*access control decision function*): Fonction spécialisée prenant des décisions de contrôle d'accès par l'application des règles de la politique de contrôle d'accès à une demande d'accès, et l'exploitation de l'information ADI et du contexte dans lequel la demande d'accès est effectuée.

3.4.4 fonction d'application de contrôle d'accès (AEF) (*access control enforcement function*): Fonction spécialisée qui, pour chaque demande d'accès, fait partie du chemin d'accès entre un initiateur et une cible et applique la décision prise par la fonction ADF.

3.4.5 information de contrôle d'accès (ACI) (*access control information*): Toute information utilisée à des fins de contrôle d'accès, incluant l'information de contexte.

3.4.6 politique de contrôle d'accès: Ensemble des règles définissant les conditions dans lesquelles l'accès peut se dérouler.

3.4.7 règles de politique de contrôle d'accès: Règles de politique de sécurité concernant la fourniture du service de contrôle d'accès.

3.4.8 jeton de contrôle d'accès: Jeton de sécurité contenant l'information ACI.

3.4.9 demande d'accès: Opérations et opérandes faisant partie d'une tentative d'accès.

3.4.10 information de décision de contrôle d'accès d'une demande d'accès; demande d'accès ADI: Information ADI dérivée d'une information ACI attachée à une demande d'accès.

3.4.11 information de contrôle d'accès d'une demande d'accès; demande d'accès ACI: Information ACI sur une demande d'accès.

3.4.12 information de contrôle d'accès attachée à une demande d'accès; ACI attachée à une demande d'accès: Information ACI attachée à une demande d'accès.

3.4.13 autorisation: Information ACI attachée à l'initiateur qui peut être comparée aux étiquettes de sécurité des cibles.

3.4.14 information contextuelle: Information relative au contexte dans lequel la demande d'accès est effectuée (par exemple heure du jour) ou dérivant d'un tel contexte.

3.4.15 initiateur: Entité (personne ou mécanisme informatique par exemple) qui tente d'accéder à d'autres entités.

3.4.16 information de décision de contrôle d'accès d'initiateur; initiateur ADI: Information ADI dérivée de l'information ACI attachée à l'initiateur.

3.4.17 information de contrôle d'accès d'initiateur; information ACI initiateur: Information ACI de l'initiateur.

3.4.18 information de contrôle d'accès attachée à l'initiateur; information ACI attachée à l'initiateur: Information ACI attachée à un initiateur.

3.4.19 information de décision de contrôle d'accès d'opérande; information ADI d'opérande: Information ADI dérivée de l'information ADI attachée à l'opérande.

3.4.20 information de contrôle d'accès d'opérande; information ACI d'opérande: Information ACI sur les opérandes d'une demande d'accès.

3.4.21 information de contrôle d'accès attachée à l'opérande; information ACI attachée à l'opérande: Information ACI attachée aux opérandes d'une demande d'accès.

3.4.22 information ADI retenue: Information ADI retenue par une fonction ADF lors d'une précédente décision de contrôle d'accès pour être utilisée dans de futures décisions de contrôle d'accès.

3.4.23 cible: Entité pour laquelle un accès peut être tenté.

3.4.24 information de décision de contrôle d'accès de cible; information ADI de cible: Information ADI dérivée de l'information ACI attachée à la cible.

3.4.25 information de contrôle d'accès de cible; information ACI de cible: Information ACI relative à une cible.

3.4.26 information de contrôle d'accès attachée à la cible; information ACI attachée à la cible: Information ACI attachée à la cible.

4 Abréviations

ACI	Information de contrôle d'accès (*access control information*)
ADI	Information de décision de contrôle d'accès (*access control decision information*)
ADF	Fonction de décision de contrôle d'accès (*access control decision function*)
AEF	Fonction d'application de contrôle d'accès (*access control enforcement function*)
SI	Information de sécurité (*security information*)
SDA	Autorité du domaine de sécurité (*security domain authority*)

5 Discussion générale sur le contrôle d'accès

5.1 But du contrôle d'accès

Dans ce cadre de sécurité, le premier but du contrôle d'accès est d'éviter la menace d'opérations non autorisées impliquant un ordinateur ou un système de communication; ces menaces sont fréquemment subdivisées en classes appelées:

- utilisation non autorisée;
- divulgation;
- modification;
- destruction;
- refus de service.

Les sous-objectifs de ce cadre de sécurité sont:

- le contrôle d'accès par les processus (qui peuvent agir pour le compte d'humains ou d'autres processus) vers les données, les processus ou d'autres ressources de calculs;
- le contrôle d'accès au sein d'un domaine de sécurité ou au travers de plusieurs domaines de sécurité;
- le contrôle d'accès en fonction de son contexte; par exemple, en fonction de facteurs comme l'heure de la tentative d'accès, le lieu de l'accédant ou la route d'accès;
- le contrôle d'accès réagissant aux changements dans l'autorisation lors de l'accès.

5.2 Aspects élémentaires du contrôle d'accès

Les paragraphes suivants décrivent les fonctions abstraites de contrôle d'accès largement indépendantes des politiques de contrôle d'accès et des conceptions de systèmes. Le contrôle d'accès dans les systèmes réels concerne plusieurs types d'entités, telles que:

- les entités physiques (par exemple, systèmes réels);
- les entités logiques (par exemple, entités de couche OSI, fichiers, organisations, et entreprises);
- les usagers.

Le contrôle d'accès dans les systèmes réels peut nécessiter un ensemble d'activités complexes:

- établissement de la politique de contrôle d'accès;
- établissement des représentations de l'information ACI;
- affectation de l'information ACI aux éléments (initiateurs, cibles ou demandes d'accès);
- rattachement de l'information ACI aux éléments;
- mise à disposition de l'information ADI pour la fonction ADF;
- exécution des fonctions de contrôle d'accès;
- modification de l'information ACI (à n'importe quel moment après l'affectation des valeurs de l'information ACI; y compris la révocation);
- révocation de l'information ADI.

Ces activités peuvent être divisées en deux groupes:

- les activités opérationnelles (mise à disposition de l'information ADI pour la fonction ADF et réalisation des fonctions de contrôle d'accès);
- les activités de gestion (toutes les autres activités).

Certaines activités ci-dessus peuvent être groupées dans une seule entité identifiable au sein d'un système réel. Bien que certaines activités de contrôle d'accès précèdent nécessairement les autres, il y a souvent recouvrement et certaines activités peuvent être réalisées à plusieurs reprises.

Une présentation détaillée des notions mises en jeu dans la réalisation des fonctions de contrôle d'accès sera d'abord présentée étant donné que d'autres activités les mettent en œuvre.

5.2.1 Réalisation des fonctions de contrôle d'accès

Pour ce paragraphe, les fonctions fondamentales du contrôle d'accès sont illustrées sur les Figures 5-1 et 5-2. D'autres fonctions peuvent être nécessaires pour le fonctionnement global du contrôle d'accès. Les discussions qui suivent, présentent plusieurs façons de mettre en œuvre ces fonctions, y compris différentes façons de distribuer les fonctions de contrôle d'accès et l'information ACI, et différents styles de communication entre les fonctions de contrôle d'accès dans le même domaine de sécurité ou entre domaines de sécurité coopérants.

Les entités élémentaires et les fonctions mises en œuvre dans le contrôle d'accès sont l'initiateur, la fonction d'application de contrôle d'accès (AEF), la fonction de décision de contrôle d'accès (ADF), et la cible.

Les initiateurs représentent à la fois les êtres humains et les entités liées à l'ordinateur qui accèdent ou tentent d'accéder aux cibles. Au sein d'un système réel, un initiateur est représenté par une entité liée à l'ordinateur, bien que les demandes d'accès de l'entité liée à l'ordinateur pour le compte de l'initiateur puissent être limitées par l'information ACI de l'entité liée à l'ordinateur.

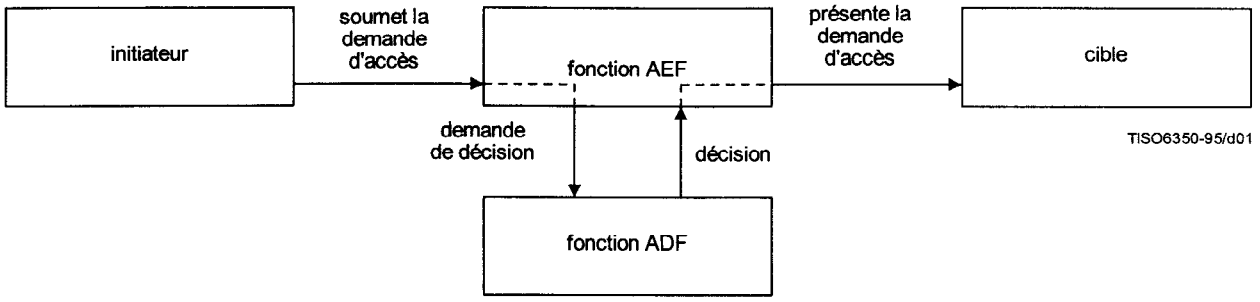

Figure 5-1 – Illustration des fonctions fondamentales du contrôle d'accès

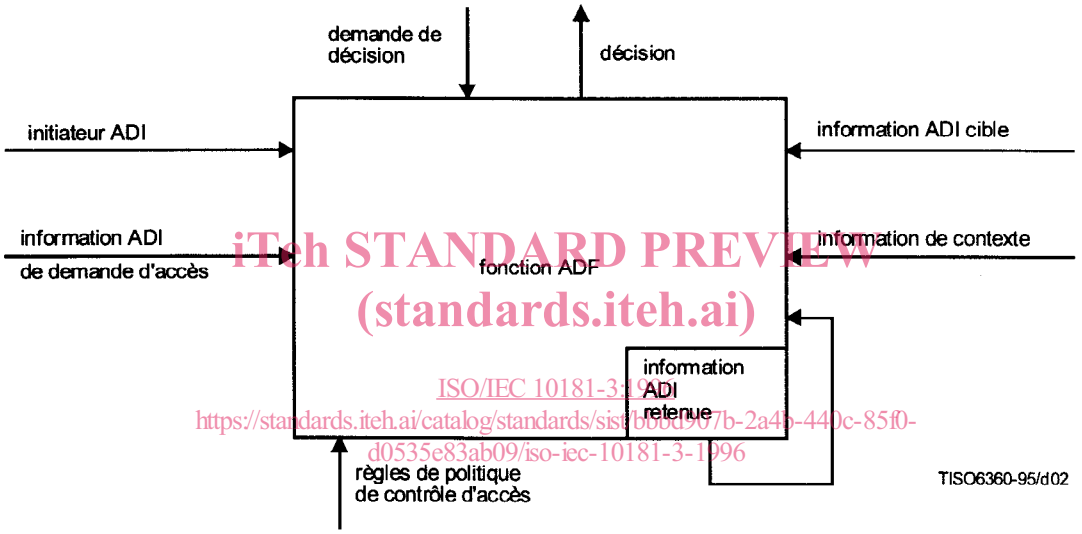

Figure 5-2 – Illustration de la fonction ADF

Les cibles représentent des entités liées au calculateur ou des entités de communication vers lesquelles l'accès est tenté ou bien les entités accédées par les initiateurs. Une cible peut, par exemple, être une entité de couche OSI, un fichier, ou un système réel.

Une demande d'accès représente les opérations et les opérandes faisant partie d'une tentative d'accès.

La fonction AEF garantit que seuls les accès légitimes de l'initiateur, déterminés par la fonction ADF, sont réalisés sur la cible. Lorsque l'initiateur effectue une demande pour réaliser un accès particulier sur la cible, la fonction AEF informe la fonction ADF qu'une décision est requise afin de prendre une résolution.

Afin de prendre une décision, la demande d'accès (en tant que partie de la demande de décision) et les types suivants d'information de décision de contrôle d'accès (ADI) sont fournis à la fonction ADF:

- ADI d'initiateur (information ADI dérivée de l'information ACI attachée à l'initiateur);
- ADI de cible (information ADI dérivée de l'information ACI attachée à la cible);
- ADI de demande d'accès (information ADI dérivée de l'information ACI attachée à la demande d'accès).

Les autres entrées de la fonction ADF sont les règles de la politique de contrôle d'accès (de l'autorité du domaine de sécurité de la fonction ADF), et toute information de contexte nécessaire pour interpréter l'information ADI ou la politique. Des exemples d'informations de contexte incluent l'emplacement de l'initiateur, l'heure d'accès, ou le chemin particulier de communications en cours d'utilisation.

Fondée sur ces entrées, et éventuellement sur l'information ADI retenue des décisions précédentes, la fonction ADF aboutit à une décision pour autoriser ou dénier l'accès tenté par l'initiateur sur la cible. La décision est transportée jusqu'à la fonction AEF qui permet ensuite à la demande d'accès d'arriver jusqu'à la cible ou qui prend d'autres actions appropriées.

Dans plusieurs cas, les demandes d'accès successives d'un initiateur sur une cible sont liées. Un exemple typique concerne une application qui ouvre une connexion vers un processus d'application cible de même niveau et ensuite tente de réaliser plusieurs accès en utilisant la même information ADI (retenue). Pour certaines demandes d'accès suivantes transmises sur la connexion, il peut être nécessaire de fournir une information ADI additionnelle à la fonction ADF afin qu'elle autorise la demande d'accès. Dans d'autres cas, une politique de sécurité peut demander que, entre un ou plusieurs initiateurs, certaines demandes d'accès liées soient sujettes à restrictions. Dans de tels cas, la fonction ADF peut utiliser l'information ADI retenue de décisions précédentes impliquant plusieurs initiateurs et cibles pour prendre une décision sur une demande d'accès particulière.

Pour ce paragraphe, une demande d'accès met en jeu une seule interaction entre un initiateur et une cible, si cela est permis par le fonction AEF. Bien que certaines demandes d'accès entre un initiateur et une cible soient simplement indépendantes, il arrive souvent que deux entités participent à un ensemble de demandes d'accès liées tel qu'un paradigme de question-réponse. Dans ces cas, les rôles d'initiateur et de cible sont assurés, comme requis, par les entités, soit simultanément soit de façon alternée, et les fonctions de contrôle d'accès sont mises en œuvre pour chaque demande d'accès, éventuellement par des composants distincts de fonction AEF, des composants de fonction ADF et des politiques de contrôle d'accès.

5.2.2 Autres activités de contrôle d'accès

5.2.2.1 Etablissement des représentations de politique de contrôle d'accès

Les politiques de contrôle d'accès sont communément définies en langages naturels sous forme de principes généraux; par exemple: seuls les responsables d'au moins un certain rang sont autorisés à examiner les informations salariales des employés. La transposition de ces principes dans des règles est une activité de conception qui précède nécessairement les autres activités de contrôle d'accès et ne fait pas partie du domaine d'application de ce cadre de sécurité. Un aperçu des concepts de politique de contrôle d'accès est donné dans l'article 6.

5.2.2.2 Etablissement des représentations des informations ACI

Dans cette activité, sont effectués les choix pour la représentation de l'information ACI au sein de systèmes réels (structure des données) et pour l'échange entre systèmes réels (syntaxes). Un grand domaine de représentations possibles est présenté dans ce cadre de sécurité. Les représentations de l'information ACI doivent être en mesure de répondre aux exigences de politiques spécifiques de contrôle de sécurité. Certaines représentations de l'information ACI peuvent être appropriées pour une utilisation à la fois dans et entre les systèmes réels. Des représentations différentes d'information ACI peuvent être utilisées à des fins différentes et entre des éléments particuliers.

Les représentations choisies pour l'information ACI peuvent être considérées comme des gabarits pour l'affectation de valeurs particulières d'information ACI à des éléments dans un domaine de sécurité (comme cela est présenté dans le paragraphe suivant). Un des aspects de l'établissement de la représentation d'information ACI concerne la détermination des types et des intervalles des valeurs de l'information ACI pouvant être assignés aux éléments dans un domaine de sécurité (mais pas les types pouvant être affectés à des éléments spécifiques).

Les représentations de l'information ACI échangée entre systèmes réels à des fins de gestion de contrôle d'accès ou pour des échanges d'information ACI entre entités et fonctions de contrôle d'accès sont candidates à la normalisation OSI. La façon dont l'information ACI est représentée au sein de systèmes réels ou est présentée à une fonction locale ADF n'est pas sujette à normalisation. La protection de l'échange d'information ACI est présentée en 7.2. Pour les applications OSI (et, éventuellement, les autres), il est approprié de considérer les représentations de l'information ACI comme des attributs consistant en des paires de la forme type d'attribut-valeur d'attribut.

5.2.2.3 Affectation de l'information ACI aux initiateurs et aux cibles

Dans cette activité, les types spécifiques d'attribut et de valeurs d'attribut de l'information ACI affectés à un élément sont désignés par une autorité SDA, ses agents, ou d'autres entités (par exemple, les propriétaires de la ressource). Ces entités peuvent, en accord avec la politique du domaine de sécurité, spécifier ou modifier l'affectation de l'information ACI.