UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T X.812

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

(11/95)

RÉSEAUX DE DONNÉES ET COMMUNICATION ENTRE SYSTÈMES OUVERTS

SÉCURITÉ

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

Recommandation UIT-T X.812

(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 n° 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.812 de l'UIT-T a été approuvé le 21 novembre 1995. Son texte est publié, sous forme identique, comme Norme internationale ISO/CEI 10181-3.

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 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

Résumé

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 DES SYSTÈMES OUVERTS – 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.

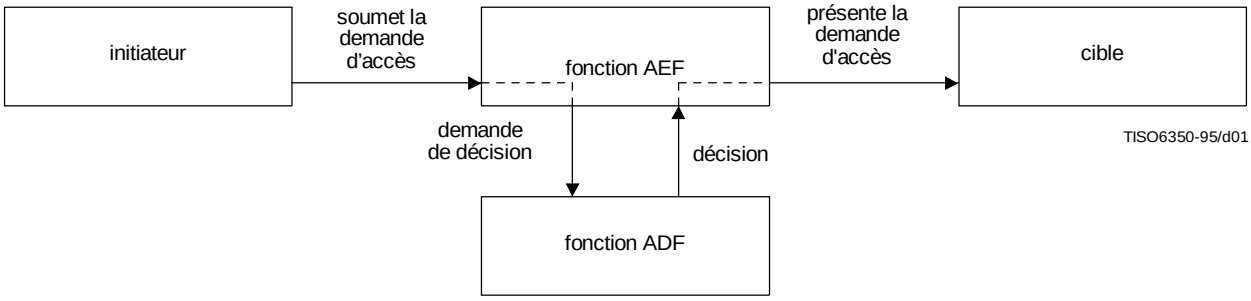

Figure 5-1 – Illustration des fonctions fondamentales du contrôle d'accès

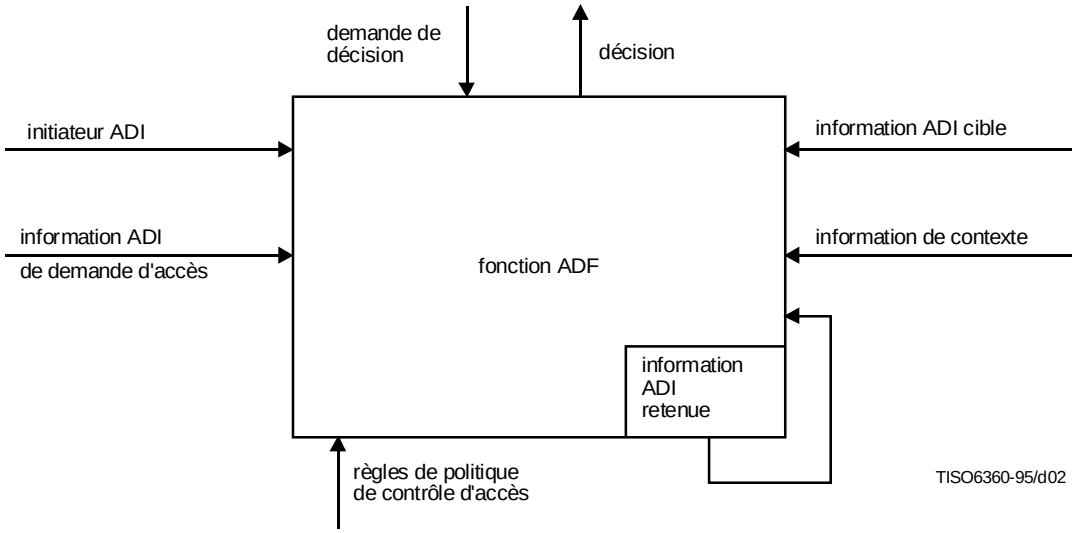

Figure 5-2 – Illustration de la fonction ADF

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.

L'information ACI affectée par une entité peut être limitée par l'information ACI qui lui a été attachée par une autre entité. L'affectation de l'information ACI aux éléments est une activité continue puisque de nouveaux éléments sont ajoutés à un domaine de sécurité.

NOTE – L'acte administratif accordant des «droits d'accès» est quelquefois appelé autorisation. Cette signification est incluse dans l'affectation de l'information ACI aux initiateurs et cibles.

L'information ACI peut être de l'information relative à une seule entité ou de l'information relative à une relation entre plusieurs entités. L'information ACI affectée à un initiateur peut être simplement relative à cet initiateur, peut être relative aux relations entre cet initiateur et des cibles particulières, ou peut être relative à des relations entre cet initiateur et des contextes possibles. Ainsi, l'information ACI affectée à un initiateur peut inclure l'information ACI de l'initiateur, l'information ACI de la cible, ou l'information de contexte. De façon similaire, l'information ACI affectée à une cible peut inclure l'information ACI de cible, l'information ACI d'initiateur (relative à un ou plusieurs initiateurs), ou l'information de contexte.

Dans une opération effective, l'information ACI doit être attachée à un élément (voir 5.2.2.4) de sorte qu'une fonction ADF utilisant l'information ADI dérivée de l'information ACI attachée ait confiance dans cette information. Ainsi, bien que l'affectation de l'information ACI aux éléments soit un préalable pour la construction de l'information ADI attachée, seule l'information ACI attachée à un élément est en réalité présente dans les systèmes ouverts réels.

5.2.2.4 Attachement de l'information ACI aux initiateurs, aux cibles et aux demandes d'accès

L'attachement de l'information ACI à un élément (par exemple, un initiateur, une cible ou une demande d'accès) crée un lien sécurisé entre l'élément et l'information ACI affectée à cet élément. L'attachement assure aux fonctions de contrôle d'accès et aux autres fonctions à la fois que l'information ACI est évidemment affectée à l'élément particulier et qu'aucune modification n'a eu lieu depuis que l'attachement a été effectué. L'attachement est réalisé en utilisant un service de sécurité. Plusieurs mécanismes d'attachement sont possibles, y compris certains mécanismes dépendant de la localisation de l'élément et de l'information ACI, alors que d'autres mécanismes peuvent dépendre de certaines signatures cryptographiques ou de certains processus de scellés. L'intégrité de l'attachement de l'information ACI aux éléments doit être protégée au sein des systèmes initiateurs et cibles (par exemple, en s'appuyant sur des fonctions de système d'exploitation comme la protection de fichier et la séparation de processus) ainsi que lors de l'échange d'information ACI. Etant donné qu'il peut y avoir plusieurs représentations possibles pour un élément de l'information ACI (à la fois au sein des systèmes et entre les systèmes), des mécanismes d'attachement différents peuvent être utilisés pour la même information ACI. Dans le cadre de certaines politiques de sécurité, la confidentialité de l'information ACI doit être maintenue.

L'attachement de l'information ACI à des éléments est une activité continue puisque de nouveaux éléments sont ajoutés à un domaine de sécurité. Une autorité SDA, son agent, ou d'autres entités autorisées, peuvent, en accord avec la politique de sécurité applicable, ajouter ou enlever, à souhait, des attachements d'information ACI. Une autorité SDA peut modifier l'information ACI attachée à un élément afin d'exprimer le changement de la politique de sécurité ou des attributs. L'information ACI attachée peut inclure des indicateurs de période de validité, minimisant ainsi l'information ACI pouvant, plus tard, être révoquée.

L'heure à laquelle l'information ACI est attachée à un élément et l'entité déclenchant le mécanisme d'attachement, dépendent du type d'élément. Les initiateurs se verront attacher l'information ACI par une autorité SDA ou son agent avant d'être capables d'effectuer les accès.

Toutes les cibles auront des informations ACI attachées par une autorité SDA ou ses agents avant de devenir accessibles. Les cibles qui sont créées par une application pour le compte d'un utilisateur ou d'une autre application auront leur information ACI attachée au moment de leur création ou après leur création. L'information ACI attachée à de telles cibles peut être restreinte par des limitations dans l'information ACI attachée à l'utilisateur ou à l'application.

Avant que l'accès ne soit tenté, l'information ACI est attachée à une demande d'accès par un utilisateur ou une application, ou par une autorité SDA ou son agent pour le compte de l'utilisateur ou de l'application. A nouveau, l'information ACI attachée à la demande d'accès peut être restreinte par les limitations de l'information ACI attachée à l'utilisateur ou à l'application. Il arrive souvent qu'une demande d'accès provoque la création d'une nouvelle entité cible (par exemple, lorsqu'un fichier est transféré entre systèmes). Une telle information ACI de cible peut être spécifiée dans (ou dérivée de) l'information ACI attachée à la demande d'accès.

5.2.2.5 Mise à disposition de l'information ADI pour la fonction ADF

Si cela est permis par la politique de contrôle d'accès et si le mécanisme d'attachement utilisé le permet, un sous-ensemble de l'information ACI attachée à un initiateur peut être choisi par l'initiateur ou la cible pour être utilisé par la fonction ADF afin de prendre une décision d'accès particulière. L'information ACI attachée à un élément peut être temporairement attachée à un autre élément, par exemple, lorsqu'une entité agit pour le compte d'une autre entité.

Afin de réaliser ses fonctions, les diverses informations ACI de la Figure 5-2 doivent être mises à disposition de la fonction ADF. Il est à noter qu'aucune supposition sur la distribution physique des entités, fonctions ou information ADI, ni sur la façon dont les entrées sont mises à disposition de la fonction ADF, n'est faite dans ce paragraphe. Certaines relations possibles entre entités et composants de contrôle d'accès distribués sont présentées dans 5.3, 5.4, et dans l'Annexe D.

Il y a trois possibilités pour l'information ADI d'initiateur, l'information ADI de cible ou l'information ADI de demande d'accès:

a) l'information ADI peut être prélocalisée dans un ou plusieurs composants de fonction ADF après l'affectation des valeurs de l'information ACI;

b) l'information ADI peut être dérivée de l'information ACI attachée fournie aux composants de la fonction ADF lors du processus de contrôle d'accès (éventuellement conjointement avec l'accès tenté);

c) l'information ADI peut être dérivée de l'information ACI attachée obtenue à partir d'autres sources (par exemple, un Agent de service d'annuaire). Soit l'initiateur ou la cible obtient l'information ACI attachée [qui est, pour la fonction ADF non dissociable de b)] ou bien la fonction ADF obtient l'information ACI attachée requise [qui pour l'initiateur ou la cible n'est pas dissociable de a)].

Les moyens par lesquels la fonction ADF obtient l'information ACI attachée et en dérive cette information ADI ne sont pas spécifiés. L'information attachée à l'initiateur n'est pas nécessairement délivrée par l'initiateur, l'information ACI attachée à la cible n'est pas nécessairement délivrée par la cible, pas plus que l'information ACI attachée à la demande d'accès n'est nécessairement délivrée avec une demande d'accès.

La fonction ADF doit être capable de déterminer, de façon univoque, que l'information ADI a été dérivée de l'information ACI attachée aux éléments par une autorité SDA appropriée. Les moyens de fournir cette garantie sont présentés dans 7.2.

5.2.2.6 Modification de l’information ACI

L'autorité SDA peut modifier l'information ACI affectée et attachée à un élément de façon à exprimer le changement des attributs de sécurité. L'information ACI peut être modifiée à n'importe quel moment après avoir été affectée aux éléments. Si la modification réduit les accès permis à un initiateur sur une cible, alors ce changement peut nécessiter la révocation de l'information ACI et de l'information ADI dérivée qui peut être retenue par les fonctions ADF.

5.2.2.7 Révocation de l'information ADI

Après révocation de l'information ACI, toute tentative d'utilisation de l'information ADI dérivée de cette information ACI doit engendrer un accès non autorisé. Toute utilisation ultérieure de l'information ADI dérivée de cette information ACI avant qu'elle n'ait été révoquée doit être évitée, ou bien sa tentative d'utilisation doit aboutir à un accès dénié. Si un accès basé sur une telle information ADI précédemment dérivée est en cours lorsque l'information ACI est révoquée, la politique de contrôle d'accès en vigueur doit exiger la fin de l'accès.

5.2.3 Envoi de l’information ACI

Dans les systèmes distribués, il est courant que des entités demandent à d'autres entités de réaliser des accès pour leur compte. Les initiateurs et les cibles sont des rôles assumés par des entités, bien que toutes les entités n'assurent pas les deux rôles. Une entité peut simultanément assumer le rôle d'initiateur au regard d'une entité tout en étant elle-même une cible pour une autre entité agissant en tant qu'initiateur.

La Figure 5-3 démontre la notion élémentaire d'une entité, A, demandant à une autre entité, B, de réaliser un accès sur encore une autre entité C. Les divers composants de contrôle d'accès qui pourraient être mis en jeu dans un tel accès chaîné ne sont pas indiqués sur la Figure 5-3.

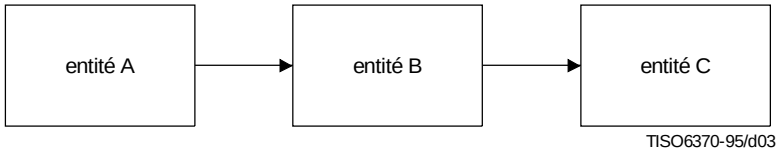

Figure 5-3 – Envoi de l'information ACI

Il y a de nombreuses variantes de cette notion élémentaire. Les variantes sont visiblement différentes dans les combinaisons de l'information ACI, requises par la politique, qui doivent exister pour autoriser le fonctionnement de tels accès chaînés et dans la façon dont l'information ACI est mise à disposition des composants de contrôle d'accès appropriés. Dans le cadre de certaines politiques, l'entité B n'a pas besoin d'informations ACI au-delà de celle qui lui est attachée pour effectuer l'accès pour l'entité A; dans le cadre d'autres politiques, l'entité B utilisera l'information ACI obtenue de l'entité A relative à l'accès; cependant dans le cas général, l'information ACI attachée aux entités A et B doit être utilisée.

Quelques exemples permettront d'indiquer quelques domaines de variations possibles.

a) Parmi les possibilités les plus simples, l'entité A pourrait demander à l'entité B d'effectuer un accès pour lequel l'information ACI est suffisante pour réaliser la demande d'accès de A.

b) L'entité A peut avoir besoin d'offrir certaines ou toutes les informations ACI nécessaires pour que la demande d'accès soit approuvée par les composants de contrôle d'accès appropriés.

   1) L'entité A pourrait offrir cette information ACI en la passant, avec la demande d'accès, à l'entité B.

   2) L'entité A pourrait demander une autorisation à C avant de demander à l'entité B d'effectuer l'accès. Dans ce cas, l'entité A fournirait l'information ACI à C qui à son tour fournirait un jeton à l'entité A. Ce jeton serait envoyé par l'entité A à l'entité C avec l'accès demandé et l'entité C reconnaîtrait alors le jeton comme l'enregistrement de l'autorisation précédente. (Se reporter à l'Annexe F pour des détails supplémentaires sur ce cas.)

La Figure 5-3 généralise cela à n'importe quel nombre d'entités intermédiaires, la fonction AEF de la dernière entité cible obtenant une décision d'accès fondée principalement sur l'information ACI obtenue d'une ou plusieurs entités faisant partie de la séquence. L'Annexe B fournit des détails supplémentaires sur les interactions entre initiateurs et cibles dans des chaînes d'accès indirect complexes.

NOTE – Le concepteur d'une politique de contrôle d'accès doit être conscient du fait que, sans précautions, de tels accès transitifs peuvent permettre des accès qui ne seraient pas directement permis.

5.3 Distribution des composants de contrôle d'accès

Une fonction AEF ou une fonction ADF peut être composée d'un ou de plusieurs composants de contrôle d'accès. Comme cela est autorisé par la politique de sécurité, les fonctions de contrôle d'accès peuvent être distribuées sur ces composants. Les fonctions élémentaires de contrôle d'accès présentées ci-dessus sont indépendantes des aspects relatifs à la localisation des composants, aux communications entre eux, ou à leur possible distribution.

Une fonction AEF est placée entre chaque instance initiateur-cible de façon que l'initiateur puisse agir sur la cible seulement par le biais de la fonction AEF. Il y a plusieurs mises en œuvre physiques possibles pour les composants de fonction AEF et ADF. Un composant de fonction ADF peut ou non être colocalisé (fortement couplé) avec un composant de fonction AEF. Un composant de fonction ADF peut servir un ou plusieurs composants de fonction ADF. De la même façon, un composant de fonction AEF peut utiliser un ou plusieurs composants de fonction ADF.

La colocalisation (fort couplage) d'un composant de fonction AEF et d'un composant de fonction ADF peut présenter des avantages en termes d'efficacité et de durée (en réduisant les délais) et peut également éviter de protéger les communications entre les fonctions AEF et ADF. Les composants de fonction ADF servant plusieurs composants de fonction AEF peuvent présenter l'avantage de réduire l'exigence de distribuer l'information ACI et rendre moins complexes certaines fonctions associées, telles que l'audit.

Une présentation des composants de fonction AEF et ADF, leur localisation et des exemples de relations s'appliquant à un seul initiateur et à une seule cible se trouvent dans l'Annexe D. Les localisations des composants peuvent être basées sur une ou plusieurs des considérations suivantes.

5.3.1 Contrôle d'accès entrant

Une autorité SDA peut considérer que le contrôle d'accès entrant au niveau d'une cible est suffisant. Dans ce cas, un composant de fonction AEF cible applique une politique de contrôle d'accès entrant et une cible ne peut pas recevoir une demande qui n'est pas en conformité avec la politique de contrôle d'accès de la cible. Cela signifie que les demandes d'accès envoyées par l'initiateur parviendront à la fonction AEF cible et seront sujettes à examen par la fonction AEF cible pour vérifier qu'elles satisfont la politique de contrôle d'accès appliquée par le composant de fonction ADF.

5.3.2 Contrôle d'accès sortant

Une autorité SDA peut considérer qu'il est important d'éviter les accès aux cibles non autorisés en employant des composants de contrôle d'accès locaux à l'initiateur (par exemple, lorsque la mise en œuvre du système de contrôle de la cible n'est pas de grande qualité, ou si les ressources réseau disponibles ne doivent pas être épuisées avant d'avoir

d'abord vérifié que la demande d'accès est autorisée), dans ce cas le contrôle d'accès sortant par une fonction AEF initiateur est nécessaire. Dans ce cas, un initiateur ne peut pas réaliser un accès qui n'est pas conforme à la politique de contrôle d'accès du domaine de sécurité initiateur.

5.3.3 Contrôle d'accès interposé

Une autorité SDA peut conclure qu'il est important de filtrer les accès entre initiateurs et cibles, dans ce cas, une fonction AEF est interposée entre l'initiateur et la cible. La fonction AEF interposée peut ensuite appliquer les politiques de contrôle d'accès entrant et sortant. Ces politiques de contrôle d'accès peuvent être indépendantes des politiques de contrôle d'accès du domaine de sécurité de l'initiateur et de la cible.

5.4 Distribution des composants de contrôle d'accès à travers des domaines de sécurité multiples

Il est possible, pour des domaines de sécurité, de participer à des relations pour lesquelles les ressources d'un domaine de sécurité peuvent être accédées depuis un autre domaine de sécurité. De multiples domaines de sécurité peuvent être mis en jeu, mais dans de nombreux cas tous ne sont pas distincts. Certains de ces domaines de sécurité contribuent à fournir l'information ACI, certains exercent le contrôle d'un accès, et certains font les deux. Ces domaines de sécurité peuvent inclure:

- le domaine de sécurité dans lequel l'information ACI est attachée à l'initiateur;
- le domaine de sécurité dans lequel réside l'initiateur;
- le domaine de sécurité dans lequel l'information ACI est attachée à la demande d'accès;
- le domaine de sécurité dans lequel l'information est attachée à la cible;
- le domaine de sécurité dans lequel réside la cible;
- les domaines de sécurité dans lesquels les décisions de contrôle d'accès sont prises;
- les domaines de sécurité dans lesquels les décisions de contrôle de sécurité sont appliquées.

Le processus de contrôle d'accès est alors similaire au cas où tous les composants de fonction AEF et ADF se retrouvent sous la même autorité SDA, comme cela est décrit dans 5.3, avec en plus les complications apportées par les relations entre autorités SDA et entre domaines et les communications entre domaines.

Les communications entre domaines comprennent:

- les notifications, entre autorités SDA ou leurs agents, de nouveaux attachements d'information ACI ou de modifications d'information ACI;
- les demandes, au moment de la tentative d'accès, de vérification et de traduction des représentations de l'information ACI et des politiques de contrôle d'accès, et les réponses à ces demandes;
- les demandes d'accès et les réponses à ces demandes.

5.5 Menaces sur le contrôle d'accès

Les informations ACI et les fonctions de contrôle d'accès peuvent être distribuées sur plusieurs systèmes réels et domaines de sécurité. L'information ACI peut être communiquée à travers des fonctionnalités de communication non sécurisées et peut être manipulée par des composants agissant sous des autorités SDA différentes. Lorsque des autorités SDA différentes sont mises en jeu, une relation de confiance entre les autorités SDA est nécessaire. Parmi les menaces qui devraient être considérées se trouvent:

- la mascarade par une entité apparaissant comme une fonction AEF ou ADF correcte;
- l'évitement d'une fonction AEF;
- l'interception, la répétition ou la modification de l'information ACI ou d'autres communications liées au contrôle d'accès;
- l'utilisation de l'information ACI par un initiateur autre que l'initiateur supposé;
- l'utilisation de l'information ACI envers des cibles autres que la cible supposée;
- l'utilisation de l'information ACI pour des demandes autres que les demandes d'accès supposées;
- l'utilisation de l'information ACI au niveau de la mauvaise fonction ADF;
- l'utilisation de l'information ACI en dehors des contraintes supposées.

Les moyens possibles pour assurer la protection contre les menaces sur le contrôle d'accès sont indiqués dans 7.2.

6 Politiques de contrôle d'accès

Les politiques de contrôle d'accès expriment des exigences de sécurité particulières dans un domaine de sécurité. Une politique de contrôle d'accès est un ensemble de règles selon lesquelles agissent les fonctions ADF. Plusieurs aspects peuvent être inclus dans des politiques de contrôle d'accès et dans leurs expressions sous forme de règles. Un ou plusieurs de ces aspects peuvent s'appliquer à une politique de sécurité particulière. Quelques mécanismes de contrôle de sécurité s'adaptent plus aisément que d'autres à des considérations particulières (se reporter à l'article 8).

NOTE – Les politiques de sécurité qui pourraient être réalisées par des mécanismes de contrôle d'accès mais qui sont relatives à d'autres mécanismes de sécurité (par exemple, confidentialité, intégrité) ne sont pas prises en compte ici.

Deux aspects importants et distincts d'une politique de contrôle d'accès concernent la façon dont elle est exprimée et la façon dont elle est gérée (6.1 et 6.2). Les politiques de contrôle d'accès appliquées administrativement sont communément exprimées et mises en œuvre en utilisant des étiquettes de sécurité, alors que les politiques de contrôle d'accès sélectionnées par les utilisateurs sont exprimées et mises en œuvre de façons différentes. Néanmoins, l'expression de la politique de contrôle d'accès, sa gestion, et les mécanismes utilisés pour la mettre en œuvre sont logiquement indépendants les uns des autres.

6.1 Expression de la politique de contrôle d'accès

6.1.1 Catégories de politiques de contrôle d'accès

Deux catégories de politique de sécurité, fondée sur les règles et fondée sur l'identité, sont identifiées dans la Rec. X.800 du CCITT | ISO 7498-2. Les politiques de contrôle de sécurité fondées sur les règles sont supposées s'appliquer à toutes les demandes d'accès d'un initiateur sur n'importe quelle cible d'un domaine de sécurité. Les politiques de contrôle d'accès fondées sur l'identité sont fondées sur des règles spécifiques à un initiateur individuel, à un groupe d'initiateurs, à des entités agissant pour le compte d'initiateurs, ou à des émetteurs agissant dans un rôle spécifique. Le contexte peut modifier des politiques de contrôle d'accès fondées sur les règles ou fondées sur l'identité. Des règles de contexte peuvent définir la totalité de la politique en vigueur. Les systèmes temps réels emploieront habituellement une combinaison de ces types de politiques; si une politique fondée sur les règles est utilisée, alors une politique fondée sur l'identité est habituellement également en vigueur.

6.1.2 Groupes et rôles

Les politiques de contrôle d'accès définies en termes de groupe d'initiateurs ou en termes d'initiateurs agissant dans des rôles spécifiques sont des types particuliers de politiques fondées sur l'identité.

Un groupe est un ensemble d'initiateurs dont les membres sont considérés équivalents lorsqu'une politique de contrôle d'accès est appliquée. Les groupes permettent à un ensemble d'initiateurs l'accès à des cibles particulières sans nécessiter l'inclusion de l'identité d'initiateurs individuels dans l'information ACI de cible, et sans affecter explicitement la même information ACI à chaque initiateur. La composition d'un groupe est déterminée par une action de gestion; la capacité de créer ou de modifier les groupes doit être sujette au contrôle d'accès. L'audit des demandes d'accès du groupe sans distinction des membres peut être ou non nécessaire.

Un rôle caractérise les fonctions que l'utilisateur est autorisé à réaliser au sein d'une organisation. Un rôle donné peut être appliqué à un seul individu (par exemple, directeur d'un département) ou plusieurs individus (par exemple, caissier, responsable des prêts, membre du conseil).

Les groupes et les rôles peuvent être utilisés hiérarchiquement pour combiner les identités des initiateurs, les groupes et les rôles.

6.1.3 Etiquettes de sécurité

Les politiques de contrôle de sécurité définies en termes d'étiquettes de sécurité sont des types particuliers de politiques de sécurité fondées sur les règles. Les initiateurs et les cibles sont associés séparément aux étiquettes de sécurité. Les décisions d'accès sont fondées sur une comparaison des étiquettes de sécurité de l'initiateur et de la cible. Ces politiques sont exprimées par des règles décrivant les accès pouvant se dérouler entre les initiateurs et les cibles ayant des étiquettes de sécurité spécifiques.

L'expression des politiques de contrôle d'accès en termes d'étiquettes de sécurité est particulièrement utile lorsqu'elle est utilisée pour fournir une forme d'intégrité ou de confidentialité.

6.1.4 Politiques de contrôle de sécurité d'initiateurs multiples

Il y a plusieurs politiques de contrôle d'accès formulées en termes d'initiateurs multiples. Ces politiques pourraient identifier des initiateurs individuels, ou des initiateurs membres du même groupe ou de groupes différents, ou d'initiateurs assumant des rôles différents, ou une combinaison de ces cas. Des exemples de telles politiques de contrôle d'accès à parties multiples sont:

- des individus spécifiquement identifiés doivent s'accorder sur un accès à réaliser. Le plus souvent les initiateurs assumant des rôles particuliers doivent s'accorder sur un accès, par exemple un président de société et un trésorier;
- deux membres de groupes différents doivent s'accorder sur un accès, par exemple un responsable de société et n'importe quel membre du conseil des directeurs. Dans cet exemple, la politique nécessiterait probablement que le même individu ne puisse pas agir pour les deux groupes, les identités individuelles et les membres du groupe feraient ainsi partie de l'information ADI utilisée par la fonction ADF;
- un nombre spécifié de membres d'un groupe (peut être la majorité) doit s'accorder sur un accès.

6.2 Gestion de la politique

Ce paragraphe identifie trois aspects dans un spectre de politique de gestion.

6.2.1 Politiques fixes

Les politiques fixes sont celles qui s'appliquent tout le temps et qui ne peuvent pas être changées, car, par exemple, elles sont inscrites dans le système.

6.2.2 Politiques appliquées administrativement

Les politiques appliquées administrativement sont celles qui sont appliquées tout le temps et peuvent être changées seulement par des personnes dûment autorisées.

6.2.3 Politiques sélectionnées par l'utilisateur

Les politiques sélectionnées par l'utilisateur sont celles qui sont disponibles à la demande d'un initiateur ou d'une cible et sont appliquées seulement pour des demandes d'accès mettant en jeu cet initiateur ou cette cible, ou les ressources de cet initiateur ou de cette cible.

6.3 Finesse et inclusion

Les politiques de contrôle d'accès peuvent définir des cibles à différents niveaux de finesse. Chaque niveau de finesse peut avoir sa propre politique logiquement séparée et peut entraîner l'utilisation de composants de fonction AEF et ADF (bien qu'ils puissent utiliser la même information ADI). Par exemple, l'accès à un serveur de base de données pourrait être contrôlé seulement au niveau du serveur; c'est-à-dire, soit un initiateur se voit dénier entièrement l'accès soit il est autorisé à accéder à tout ce qui se trouve dans le serveur. D'une autre façon, l'accès pourrait être contrôlé au niveau des fichiers individuels, des enregistrements des fichiers, ou même des éléments de données des enregistrements. Une base de données particulière pourrait être constituée par un arbre d'information d'annuaire, l'accès à celui-ci pourrait être contrôlé au niveau de finesse de l'arbre complet, ou de sous-arbres au sein de l'arbre, ou d'entrées dans l'arbre, ou même de valeurs d'attributs dans les entrées. Un autre exemple de finesse est un système de calcul et les applications au sein du système.

L'inclusion peut être utilisée pour contrôler l'accès à un ensemble de cibles en spécifiant une politique permettant l'accès à ces cibles seulement si l'accès à une cible les contenant est autorisé. L'inclusion pourrait également être appliquée à des sous-groupes d'initiateurs contenus dans un groupe plus grand. L'inclusion est souvent appliquée à des cibles liées entre elles, comme les fichiers d'une base de données ou les éléments de données des enregistrements. Dans le cas d'un élément contenu dans un autre, il est nécessaire que le droit d'accès requis pour «passer à travers» les éléments inclus soit donné à l'initiateur avant qu'il tente d'accéder à un élément inclus. A moins que les concepteurs de ces politiques de sécurité y prennent garde, un accès dénié par une politique peut, lorsque cela n'est pas intentionnel, être effectivement autorisé par une autre.

6.4 Règles d'héritage

Un nouvel élément peut être créé en copiant un élément existant, en changeant un élément existant, en combinant des éléments existants, ou par construction. L'information ACI du nouvel élément peut dépendre de facteurs comme

l'information ACI de son créateur ou l'information ACI des éléments copiés, modifiés ou fusionnés. Bien que le créateur de l'élément puisse être autorisé à restreindre plus avant son information ACI, des règles d'héritage spécifient ces dépendances des informations ACI.

Les règles d'héritage font partie d'une politique de contrôle d'accès qui détermine la création et la modification de l'information ACI, ou l'application indirecte de l'information ACI à un élément en fonction de son appartenance à un domaine de sécurité ou par l'inclusion d'une cible dans une autre.

Des règles d'héritage peuvent ou non être elles-mêmes héritées par des éléments copiés, modifiés ou fusionnés. Un initiateur peut être autorisé à copier une cible pour sa propre utilisation, mais peut se voir interdire de faire plus de copies ou d'autoriser d'autres initiateurs à la copier ou à l'utiliser. D'une autre façon, une fois qu'une copie est effectuée, il peut ne pas y avoir de contrôle sur les utilisations ultérieures.

Lorsqu'un élément est contenu dans un autre, certaines de (toutes) ses informations ACI peuvent être déduites, en fonction des règles d'héritage, de l'information ACI des éléments contenants. De telles règles d'héritage peuvent simplifier l'administration de politiques uniformes appliquées à un grand nombre d'éléments.

6.5 Priorités entre règles de politique de contrôle d'accès

Il est possible que des règles de politique de contrôle d'accès soient en conflit. Les règles de priorité spécifient l'ordre selon lequel les règles de politique de contrôle d'accès sont appliquées et quelles sont les règles qui ont priorité sur les autres. Par exemple si les règles A et B d'une politique de contrôle de sécurité amèneraient individuellement une fonction ADF à une décision différente pour un accès demandé, une règle de priorité pourrait donner la priorité à la règle A, dans ce cas la règle B ne serait pas considérée, ou la règle de priorité pourrait nécessiter que les deux règles autorisent l'accès de la requête.

Les règles de priorité peuvent, lorsqu'un initiateur agit comme membre du groupe ou dans un rôle particulier, être appliquées à l'utilisation de l'information ACI attachée à l'initiateur. La règle de priorité pourrait autoriser l'information ACI propre à l'initiateur à être combinée avec l'information ACI du groupe ou du rôle assumé, dans ce cas elle doit également spécifier comment les informations ACI en conflit sont combinées. D'une autre façon, la règle de priorité pourrait nécessiter que seule l'information ACI de rôle ou de groupe soit appliquée à une demande d'accès particulière.

Dans les cas où une demande d'accès met en jeu des domaines de sécurité multiples, les principes décrits dans la Rec. X.810 | ISO/CEI 10181-1 relatifs aux politiques d'interaction sécurisée doivent être respectés.

6.6 Règles de politique de contrôle de sécurité par défaut

Une politique de contrôle de sécurité peut inclure des règles de politique de contrôle d'accès par défaut. Cela pourrait être utilisé lorsqu'un ou plusieurs initiateurs n'ont pas explicitement concédé ou dénié l'accès à une cible spécifique. Par exemple, une règle de politique de contrôle d'accès par défaut pourrait permettre l'accès à une cible si l'accès n'est pas explicitement interdit par d'autres règles de politique de contrôle de sécurité appliquées à l'information ACI concernée.

6.7 Correspondance de politique par le biais de domaines de sécurité coopérants

Lors de la fourniture du contrôle d'accès pour des demandes d'accès entre domaines de sécurité coopérants, il y aura quelquefois besoin de faire correspondre ou de traduire l'information ACI attachée à la demande d'accès. Il peut en résulter des domaines coopérants ayant des représentations différentes pour l'information ACI, ou des interprétations différentes de la politique de sécurité pour la même information ACI. Des exemples d'informations qui pourraient être mises en correspondance entre des domaines de sécurité coopérants comprennent:

- identificateurs d'individu, de groupe, ou de rôle (par exemple, l'individu JSmith dans le domaine de sécurité X peut être reconnu comme l'individu XJSmith dans le domaine de sécurité Y);
- les rôles et leurs attributs (par exemple, *l'administrateur de sécurité* dans un réseau privé attaché à un transporteur public peut être reconnu comme *un administrateur de sécurité de l'abonné* dans le réseau public du transporteur);
- les identificateurs d'individu, du rôle ou du groupe (par exemple, tous les individus dans un réseau privé peuvent être mis en correspondance avec le rôle de l'abonné individuel dans un réseau public du transporteur).

7 Information de contrôle d'accès et fonctionnalités

7.1 Information ACI

Les types d'information ACI incluent l'initiateur, la cible, la demande d'accès, l'opération, l'opérande et l'information de contexte, décrits dans cet article. Il peut être nécessaire d'échanger l'information ACI entre systèmes réels en tant qu'élément de la fonction de contrôle d'accès. Lors de tels échanges, il est essentiel que les entités coopérantes aient une compréhension mutuelle de la syntaxe abstraite. La présentation de l'information ACI dans cet article fournit la base d'une description détaillée de structures particulières de contrôle d'accès décrites dans l'article 8.

NOTE – Afin de maximiser l'interopérabilité entre systèmes réels, il a besoin de normaliser les représentations de l'information ACI. Les autres informations ACI qu'il n'est pas jugé nécessaire de normaliser (par exemple, l'information ADI retenue), ne sont pas couvertes dans cet article.

Il sera nécessaire de définir l'information ACI requise, en fonction de la politique de sécurité choisie.

7.1.1 Information ACI d'initiateur

L'information ACI d'initiateur est l'information ACI relative à un initiateur.

Des exemples de contenu d'information ACI d'initiateur incluent:

a) l'identité de contrôle d'accès d'un individu;

b) l'identificateur du groupe hiérarchique dans lequel la qualité de membre est revendiquée;

c) l'identificateur du groupe fonctionnel dans lequel la qualité de membre est revendiquée;

d) identificateurs des rôles pouvant être pris;

e) marquage de la sensibilité;

f) marquage de l'intégrité.

NOTE – Une identité individuelle de contrôle d'accès n'est pas nécessairement la même que celle utilisée pour l'authentification, l'audit ou la facturation. L'identité individuelle de contrôle d'accès est unique au sein de l'espace de nom de l'autorité SDA (se reporter à l'Annexe C).

7.1.2 Information ACI de cible

L'information ACI de cible est l'information ACI relative à une cible.

Des exemples d'information ACI de cible incluent:

a) identité de contrôle d'accès d'une cible;

b) marquage de sensibilité;

c) marquage d'intégrité;

d) identificateur du récepteur contenant une cible.

7.1.3 Information ACI de demande d'accès

L'information ACI de demande d'accès est l'information ACI relative à une demande d'accès.

Des exemples d'information ACI de demande d'accès incluent:

a) classes d'opérations autorisées (par exemple, lecture, écriture);

b) niveau d'intégrité nécessaire pour l'utilisation de l'opération;

c) type des données de l'opération.

7.1.4 Opérande de l'information ACI

L'information ACI d'opérande est l'information ACI relative à un opérande de demande d'accès.

Des exemples d'information d'opérande comprennent:

a) marquages de sensibilité;

b) marquages d'intégrité.

7.1.5 Information de contexte

Des exemples d'information de contexte comprennent:

a) intervalles de temps: un accès peut être concédé seulement durant des intervalles précis spécifiés par jour, semaines, mois, années, etc.;

b) route: un accès peut être concédé seulement si la route utilisée a des caractéristiques spécifiques;

c) emplacement: un accès peut être concédé seulement pour des initiateurs situés sur des systèmes spécifiques, stations de travail ou terminaux, ou seulement à des initiateurs situés à un emplacement physique spécifique;

d) état du système: un accès peut être concédé pour une information ADI particulière seulement lorsque le système est dans un état particulier (par exemple, durant une période de récupération de catastrophe);

e) teneur de l'authentification: un accès peut seulement être concédé lorsque les mécanismes d'authentification d'au moins une solidité donnée sont utilisés;

f) d'autres accès actuellement actifs pour cet initiateur ou pour d'autres initiateurs.

7.1.6 Information ACI attachée à l'initiateur

L'information ACI attachée à l'initiateur peut contenir l'information ACI d'initiateur, certaines informations ACI de cible et de l'information de contexte sélectionnée. Des formes d'information ACI attachée à l'initiateur sont présentées dans l'article 8, comme les étiquettes de sécurité, les capacités, et les certificats de contrôle d'accès. Des exemples comprennent:

a) ACI d'initiateur;

b) une identité de contrôle d'accès de cible et les accès autorisés sur la cible (par exemple, une capacité);

c) emplacement de l'initiateur.

7.1.7 Information ACI attachée à la cible

L'information ACI attachée à la cible peut contenir certaines informations ACI d'initiateur, des informations ACI de cible et de l'information de contexte sélectionnée. Des formes d'information ACI attachée à la cible sont présentées dans l'article 8, comme les étiquettes et les listes de contrôle d'accès. Des exemples comprennent:

a) identités de contrôle d'accès d'initiateur individuel et les accès qui leur sont autorisés ou déniés sur la cible;

b) identités de contrôle d'accès de membre de groupe hiérarchique et les accès qui leur sont autorisés ou déniés sur la cible;

c) identités de contrôle d'accès de membre de groupe fonctionnel et les accès qui leur sont autorisés ou déniés sur la cible;

d) identités de contrôle d'accès de rôle et les accès qui leur sont autorisés ou déniés sur la cible;

e) autorités et les accès qui leur sont autorisés.

7.1.8 Information ACI attachée à la demande d'accès

L'information ACI attachée à la demande d'accès peut contenir une information ACI d'initiateur, une information ACI de cible et de l'information de contexte. Des exemples comprennent:

a) paires initiateur/cible autorisées à prendre part à un accès;

b) cibles autorisées à prendre part à un accès;

c) initiateurs autorisés à prendre part à un accès.

7.2 Protection de l'information ACI

7.2.1 Certificats de contrôle d'accès

L'information ACI échangée entre systèmes réels nécessite une protection contre une variété de menaces sur le contrôle d'accès présentée dans 5.5. L'autorité sous laquelle l'information ACI a été émise doit être vérifiable par une fonction ADF qui utilise l'information ADI qui en est dérivée. Un moyen de fournir cette vérification consiste à envelopper l'information ACI dans un certificat de sécurité signé ou scellé par l'autorité émettrice. Une telle enveloppe est appelée certificat de sécurité.

Un certificat de contrôle d'accès peut contenir des informations de diverses formes. Plusieurs sont communes pour la protection des certificats en général et sont présentées dans la Rec. UIT-T X.810 | ISO/CEI 10181-1.

Les éléments d'information suivants spécifiques à l'initiateur peuvent être inclus:

- information ACI d'initiateur;
- un moyen de valider l'attachement du certificat de contrôle de sécurité pour un initiateur spécifique afin qu'il ne puisse pas être utilisé par un autre initiateur;
- un identificateur de compte sur lequel l'accès sera facturé;
- des identificateurs d'entités comptables (par exemple, responsable) pour l'accès à des fins de facturation ou d'audit;
- le nombre de fois où le certificat de contrôle d'accès peut être utilisé par un initiateur particulier.

Les éléments de données suivants spécifiques à une cible peuvent être inclus:

- information ACI de cible;
- un moyen de valider l'attachement du certificat de contrôle de sécurité à une cible spécifique afin qu'il ne puisse pas être utilisé par une autre cible;
- le nombre de fois où le certificat de contrôle d'accès peut être utilisé par un initiateur particulier.

Les éléments de données suivants spécifiques à une demande d'accès peuvent être inclus:

- un moyen de valider l'attachement du certificat de contrôle de sécurité à une demande d'accès spécifique afin qu'il ne puisse pas être utilisé par un autre initiateur;
- un moyen de valider l'attachement du certificat de contrôle de sécurité à une ou plusieurs demandes d'accès afin qu'il ne puisse pas être utilisé avec d'autres demandes d'accès (par exemple, pour l'envoi de la demande d'accès);
- le nombre de fois où le certificat de contrôle d'accès peut être utilisé pour accéder à une cible particulière;
- information ACI de demande d'accès.

7.2.2 Jetons de contrôle d'accès

Un autre moyen général de protéger l'information ACI consiste à la placer dans un jeton de sécurité. Un jeton de sécurité, à la différence d'un certificat de contrôle d'accès qui est signé ou scellé par une autorité, peut être produit par l'initiateur. Dans le cas d'un contrôle d'accès, un jeton d'accès est particulièrement important pour l'information ACI attachée à la demande.

Un certificat de contrôle d'accès peut être obtenu d'une autorité SDA pour être utilisé dans plusieurs demandes. Cependant, l'initiateur peut générer un jeton de sécurité pour attacher le certificat de contrôle d'accès à une demande d'accès spécifique.

Un jeton de sécurité peut contenir des informations de formes diverses. Plusieurs de ces informations sont communes à la protection des jetons de sécurité en général et sont présentées dans la Rec. UIT-T X.810 | ISO/CEI 10181-1.

Les mêmes éléments de données spécifiques à l'initiateur, à la cible, et à la demande d'accès pouvant être inclus dans un certificat de contrôle d'accès peuvent être également inclus dans un jeton de contrôle d'accès.

7.3 Fonctionnalités de contrôle d'accès

Ce paragraphe identifie plusieurs fonctionnalités de contrôle d'accès qui peuvent être utilisées pour assurer le contrôle d'accès dans les systèmes réels. Les descriptions génériques des fonctionnalités de contrôle d'accès fournies ne sont pas dépendantes de mécanismes spécifiques. Les primitives spécifiques d'interface à utiliser au sein de systèmes réels particuliers ne sont pas imposées.

NOTE – Bien que les fonctionnalités de contrôle d'accès soient décrites de manière générique, elles visent à illustrer, parmi les différentes approches possibles, une approche générale pour la fourniture du service de contrôle d'accès.

Les fonctionnalités de contrôle d'accès se répartissent en celles liées à la gestion qui peuvent être déclenchées, par exemple, par un administrateur de sécurité, et en celles liées à l'exploitation du contrôle d'accès. En particulier, les fonctionnalités liées à la gestion mettent en œuvre les activités «attachement de l'information ACI aux éléments», décrite dans 5.2.2.4, «modification de l'information ACI», décrite dans 5.2.2.6, et «révocation de l'information ACI», décrite dans 5.2.2.7. Les fonctionnalités liées à l'exploitation mettent en œuvre les activités «mise à disposition de l'information ACI pour la fonction ADF», décrite dans 5.2.2.5, et «réalisation des fonctions de contrôle d'accès», décrite dans 5.2.1. Lorsque différents systèmes réels ou domaines de sécurité utilisent des représentations d'information ACI différentes, des fonctionnalités additionnelles sont nécessaires pour mettre en correspondance les représentations.

7.3.1 Fonctionnalités liées à la gestion

Parmi les activités du 5.2.2, l'établissement de la politique et des représentations de l'information ACI ainsi que l'affectation de l'information ACI aux éléments ne sont pas traités ici. La fonctionnalité Installer l'information ACI est liée à l'attachement de l'information ACI aux éléments. Les fonctionnalités Changer l'information ACI et Révoquer l'information ACI sont liées à la modification et la révocation de l'information ACI. Les fonctionnalités pour mettre en service et hors service les composants de contrôle d'accès et pour lister les informations ACI d'un élément viennent en supplément des activités identifiées dans 5.2.1.

- Installer l'information ACI – Cette fonctionnalité attache un ensemble initial d'informations ACI (par exemple, des capacités à l'usage des initiateurs, les étiquettes de sécurité à l'usage des initiateurs et des cibles, et les listes ACL pour les cibles) à un élément.
- Changer l'information ACI – Cette fonctionnalité modifie (par exemple, ajoute ou enlève de) l'information ACI attachée à un élément.
- Révoquer l'information ACI – Cette fonctionnalité révoque l'utilisation de l'information ACI attachée à un élément afin que l'information ACI ne soit plus significative pour cet élément. Cela est différent de Changer l'information ACI car toute information ADI relative à cette information ACI est également révoquée.
- Révoquer l'information ADI retenue – Cette fonctionnalité révoque la validité de l'information ADI retenue.
- Lister l'information ACI – Cette fonctionnalité liste l'information ACI désignée et attachée à un élément donné.
- Composant de mise hors service – Cette fonctionnalité met hors d'utilisation un composant de fonction de contrôle d'accès. Dans le cas d'un composant de fonction AEF, la fonctionnalité inhibe tous les accès à travers ce composant de fonction AEF (cela évite tout accès à des cibles exclusivement desservies par ce composant de fonction AEF).
- Composant de remise en service – Cette fonctionnalité remet en service un composant de fonction de contrôle d'accès.

7.3.2 Fonctionnalités relatives à l'exploitation

Les fonctionnalités relatives à l'exploitation sont supposées être utilisées de la façon suivante, cependant toute interaction de contrôle d'accès ne nécessitera pas toutes ces étapes:

a) l'initiateur de la première demande d'accès d'une activité détermine, pour les éléments mis en jeu dans l'activité, l'autorité SDA en utilisant la fonctionnalité Identifier les autorités de sécurité de confiance (voir la Rec. UIT-T X.810 | ISO/CEI 10181-1);

b) une politique d'interaction sécurisée est établie pour être utilisée dans l'activité (voir la Rec. UIT-T X.810 | ISO/CEI 10181-1);

c) l'information ACI est attachée aux éléments, comme cela est décrit dans 5.2.2.4, en utilisant les fonctionnalités Acquérir et Générer l'information ACI;

d) l'information ADI est mise à disposition de la fonction ADF par le biais de l'utilisation du dispositif Vérifier l'information ACI attachée et Dériver l'information ADI;

e) l'information de contexte, requise par la politique d'interaction sécurisée, est obtenue en utilisant la fonctionnalité Obtenir l'information de contexte;

f) la décision de contrôle d'accès est obtenue par le biais du dispositif Décider l'accès.

Plusieurs des fonctionnalités décrites ci-dessous utilisent, comme cela est présenté dans 7.2, l'information ACI protégée (pour assurer l'intégrité ou la confidentialité requise par la politique de sécurité).

7.3.2.1 Acquérir l'information ACI attachée à l'initiateur

Cette fonctionnalité obtient, avant une demande d'accès, l'information ACI attachée à l'initiateur, un certificat de contrôle d'accès ou un jeton de contrôle d'accès contenant l'information ACI attachée à l'initiateur.

Déclenchée par un initiateur ou une fonction ADF.

Les entrées possibles sont:

- identité authentifiée de l'initiateur (obtenue à partir du dispositif Vérifier décrit dans la Rec. UIT-T X.811 | ISO/CEI 10181-2);
- critères de sélection de l'information ACI attachée à l'initiateur;

- période de validité;
- identité d'une cible ou d'un groupe de cibles;
- politique d'interaction sécurisée.

Les sorties possibles sont:

- état (succès ou échec du dispositif Acquérir l'information ACI attachée à l'initiateur);
- information ACI attachée à l'initiateur ou certificat de contrôle d'accès ou jeton de contrôle d'accès contenant l'information ACI attachée à l'initiateur.

7.3.2.2 Acquérir l'information ACI attachée à la cible

Cette fonctionnalité obtient l'information ACI attachée à la cible.

Déclenchée par la fonction ADF.

Les entrées possibles sont:

- identité de la cible;
- critères de sélection de l'information ACI attachée à la cible;
- période de validité;
- politique d'interaction sécurisée.

Des sorties possibles sont:

- état;
- information ACI attachée à la cible.

7.3.2.3 Générer l'information ACI attachée à la demande d'accès

Cette fonctionnalité attache, à une demande d'accès, l'information ACI attachée à l'initiateur, l'information ACI de demande d'accès ou l'information ACI attachée à l'opérande nécessaires pour qu'une décision de contrôle d'accès puisse être prise.

Déclenchée par l'initiateur.

Les entrées possibles sont:

- information ACI attachée à l'initiateur (un contrôle d'accès contenant l'information ACI attachée à l'initiateur ou l'information ADI retenue);
- l'information ACI attachée à l'opérande;
- identité de cible;
- opérations et opérandes;
- période de validité;
- politique d'interaction sécurisée.

Les sorties possibles sont:

- état;
- information ACI attachée à la demande d'accès;
- jeton de contrôle d'accès;
- certificat de contrôle d'accès (généré par une autorité SDA pour le compte de l'initiateur);
- information ADI retenue.

NOTE – La première demande d'accès d'une séquence de demandes d'accès peut renvoyer l'information ADI retenue pouvant être utilisée à la place de l'information ACI attachée à l'initiateur.

7.3.2.4 Vérifier l'information ACI attachée et l'information ADI dérivée

Cette fonctionnalité vérifie la validité de l'information ACI attachée et en dérive l'information ADI. Dans les cas où certaines ou toutes les informations ADI sont préstockées au niveau de l'ADF, ce service pourrait être étendu ou remplacé par la récupération d'une information ADI préstockée.

Déclenchée par la fonction ADF.

Les entrées possibles sont:

- les informations ACI attachées (initiateur, cible, demande d'accès ou opérande);
- jeton de contrôle d'accès;
- certificat de contrôle d'accès;
- opérations et opérandes;
- période de validité;
- politique d'interaction sécurisée.

Les sorties possibles sont:

- état;
- opérations et opérandes;
- informations ADI (initiateur, cible, demande d'accès, ou opérande).

7.3.2.5 Obtenir l'information de contexte

Cette fonctionnalité obtient l'information de contexte requise pour qu'une décision de contrôle d'accès soit prise.

Déclenchée par l'initiateur ou la fonction ADF.

Les entrées possibles sont:

- opérations et opérandes;
- information de contexte requise;
- politique d'interaction sécurisée.

Les sorties possibles sont:

- état;
- information de contexte.

7.3.2.6 Décider l'accès

Cette fonctionnalité détermine si un accès est autorisé.

Déclenchée par la fonction ADF.

Les entrées possibles sont:

- opérations et opérandes;
- information ADI d'initiateur;
- information ADI d'opérande;
- information ADI de cible;
- information de contexte;
- information ADI retenue;
- politique d'interaction sécurisée.

Les sorties possibles sont:

- décisions de contrôle d'accès;
- période de validité de la décision;
- séquence des demandes d'accès autorisées;
- information ADI retenue.

8 Classification des mécanismes de contrôle d'accès

8.1 Introduction

Un mécanisme de contrôle d'accès est basé sur une structure de contrôle d'accès (par exemple fondée sur des listes de contrôle d'accès, capacités, étiquettes, et contexte) et des mécanismes de support pour fournir, dans le cadre de cette structure, l'information ADI à la fonction ADF. Cet article décrit une gamme de structures de contrôle d'accès définies en

termes d'informations ACI devant être gardées en différents lieux (principalement au niveau de l'initiateur ou de la cible) et les mécanismes de support courants utilisés dans la fonctionnalité Décider l'accès du 7.3.2.6. Une structure élémentaire et des variantes courantes ou probables de ces structures sont décrites.

Cet article présente les principales catégories de mécanismes et de structures de contrôle d'accès; son objectif est d'indiquer que des structures différentes, chacune ayant ses propres avantages et désavantages, peuvent entrer dans un cadre unificateur. Les structures de contrôle d'accès typiques peuvent être définies de la façon suivante en termes d'information ACI attachée à l'initiateur et attachée à la cible:

a) si, dans le cadre d'une politique de contrôle de sécurité, on considère un ensemble de couples (identité de cible, type d'opération) comme une information ACI attachée à l'initiateur, et les identités de la cible comme une information ACI attachée à la cible, on obtient ce qui, par essence, est une structure de capacité;

b) si, dans le cadre d'une politique de contrôle appropriée, on considère ce qui est communément appelé «autorisation» et «classification» comme une information ACI attachée respectivement à l'initiateur et à la cible on obtient ce qui, par essence, est une structure fondée sur l'étiquette;

c) si, dans le cadre d'une politique appropriée de contrôle d'accès, on considère une identité d'initiateur en tant qu'information ACI attachée à l'initiateur, et un ensemble de couples (identité d'initiateur, type d'opération) en tant qu'information ACI attachée à la cible on obtient ce qui, par essence, est une structure de listes de contrôle d'accès;

d) les règles concernant l'information de contexte sont le plus souvent utilisées conjointement avec d'autres structures de contrôle d'accès, mais elles peuvent être utilisées seules pour créer une structure de contrôle d'accès fondée sur le contexte. L'information de contexte peut faire partie de l'information ACI attachée à l'initiateur, de l'information ACI attachée à la demande d'accès ou de l'information ACI attachée à la cible, ou bien elle peut être mise à disposition de la fonction ADF indépendamment d'autres informations ACI.

Il est facile de concevoir des variantes de a), ci-dessus, plus sophistiquées, donnant à la fonctionnalité un plus grand domaine d'application, dans lesquelles l'identité de cible devient un type de cible avec plus d'une cible possédant un «type» d'attribut donné. Une étape de plus permet de considérer ce «type» d'attribut comme une «autorisation» comparée à une étiquette de sécurité, et ainsi aboutir à b) ci-dessus. De la même façon chacune des trois premières structures peut être considérée comme des exemples de leur structure voisine. Chaque structure peut être vue en tant que différentes parties d'un continuum dans lequel les structures se recouvrent et ne sont pas totalement séparées.

Lorsque les noms d'initiateurs sont gardés au niveau de la cible pour utilisation en tant qu'information ACI attachée à la cible (par exemple, entrées dans la liste ACL), la gestion au jour le jour d'informations ACI attachées à la cible est difficile pour les systèmes ayant une population dynamique d'initiateurs. Inversement, lorsque les noms des cibles sont gardés comme information ACI attachée à l'initiateur (par exemple, dans les capacités) la gestion au jour le jour d'informations ACI attachées à l'initiateur est difficile pour les systèmes des populations dynamiques de cible.

Ainsi, il apparaît clairement que la gestion est un facteur qui devrait influencer les choix relatifs à l'expression de la politique, et que la définition d'une norme pour tous les systèmes basés sur une approche ou une autre n'est pas appropriée. Un système pratique nécessitera probablement plusieurs structures de contrôle d'accès issues de différents endroits dans le spectre.

8.2 Structure de liste ACL

8.2.1 Caractéristiques élémentaires

Les caractéristiques élémentaires de la structure de contrôle d'accès sont:

a) le contrôle d'accès est géré comme une liste de paires (qualificatif d'initiateur, qualificatif d'opération) en tant qu'informations ACI attachées à la cible et les identificateurs d'individus, de groupe ou de rôle en tant qu'informations ACI attachées à l'initiateur;

b) cette classe de contrôle d'accès est pratique lorsqu'un bon niveau de finesse du contrôle d'accès est requis;

c) cette classe de contrôle d'accès est pratique lorsqu'il y a peu d'initiateurs ou de groupements d'initiateurs;

d) cette classe de contrôle d'accès est pratique pour révoquer l'accès à une cible ou à un groupe de cibles;

e) cette classe de contrôle d'accès est pratique lorsque la gestion du contrôle d'accès est réalisée sur une base cible par cible plutôt que initiateur par initiateur;

f) cette classe de contrôle d'accès n'est pas pratique lorsque la population d'individus ou de groupes d'initiateurs change fréquemment, mais elle est pratique lorsque les populations de cible sont dynamiques.

8.2.2 Information ACI

8.2.2.1 Information ACI attachée à l'initiateur

Un identificateur d'un individu, d'un groupe ou d'un rôle constitue la principale information ACI attachée à l'initiateur dans la structure de liste ACL.

8.2.2.2 Information ACI attachée à la cible

Une liste ACL constitue la principale information ACI attachée à la cible dans la structure de la liste ACL. Une liste ACL est un ensemble ou une séquence d'entrées. Chaque entrée a deux champs:

a) *qualificatif de l'initiateur*

Dans une liste ACL simple, le qualificatif est l'identificateur caractéristique d'un initiateur auquel une «opération de qualificatif» (voir ci-dessous) est appliquée. Le qualificatif de l'initiateur peut, cependant, être moins spécifique, en représentant l'information ACI plus générale comme son rôle ou son appartenance à un groupe.

b) *qualificatif d'opération*

Cela décrit les opérations, ou les classes d'opérations (dans une demande d'accès), autorisées ou déniées pour le qualificatif de l'initiateur associé.

NOTE – En plus des opérations ou des classes d'opérations, les limitations sur les valeurs des opérandes peuvent être appliquées pour raffiner les conditions d'accès souhaitées.

8.2.3 Mécanismes de support

Deux mécanismes peuvent être utilisés pour obtenir l'information ACI attachée à l'initiateur à partir de laquelle l'information ADI, requise dans la fonctionnalité Décider l'accès, est dérivée:

a) *en utilisant l'authentification*

Si le contrôle d'accès est basé sur l'identité de l'initiateur individuel, alors l'identité peut être validée, soit directement soit indirectement, en utilisant l'authentification.

Si le contrôle d'accès est basé sur l'identité de rôle ou de groupe, l'identité authentifiée constitue un paramètre d'une fonctionnalité Acquérir l'information ACI attachée à l'initiateur, utilisée pour obtenir un groupe ou un rôle validé.

b) *en utilisant les certificats de contrôle d'accès ou les jetons de contrôle d'accès*

L'initiateur obtient un certificat de contrôle d'accès ou un jeton de contrôle d'accès (ou les deux) en utilisant la fonctionnalité Acquérir l'information ACI attachée à l'initiateur. Ce certificat ou ce jeton de contrôle d'accès est alors attaché, par l'initiateur, à une demande d'accès en utilisant la fonctionnalité Générer l'information ACI attachée à la demande d'accès et il est finalement vérifié par la fonction ADF en utilisant les fonctionnalités Vérifier l'information ACI attachée et Dériver l'information ADI.

L'acceptabilité de l'autorité du certificat identifiée dans un certificat de contrôle d'accès, ou de l'initiateur dans le cas d'un jeton de contrôle d'accès, fait partie des fonctionnalités Vérifier l'information ACI attachée et Dériver l'information ADI.

L'information ADI d'initiateur (par exemple, les identificateurs d'individu, de groupe ou de rôle), l'information ADI de demande d'accès et de cible (par exemple, le qualificatif de demande d'accès) sont les paramètres du dispositif Décider l'accès. L'information ADI d'initiateur et l'opération dérivée de la demande d'accès sont comparées, en utilisant l'algorithme de correspondance, avec chaque entrée (qualificatif d'initiateur, qualificatif de demande d'accès) de la liste de contrôle d'accès. La décision de contrôle d'accès est prise sur la base de l'établissement ou non de la correspondance. La décision renvoyée indiquera que le contrôle d'accès devrait être dénié s'il y a correspondance avec une liste d'exclusions ou s'il n'y a pas de correspondance avec une liste d'inclusions. Autrement, la décision renvoyée indiquera que le contrôle d'accès devrait être accordé.

8.2.4 Variantes de cette structure

Ce paragraphe décrit des variantes courantes de la structure élémentaire de la liste de contrôle d'accès décrite ci-dessus.

8.2.4.1 Listes ACL ordonnées

Dans certaines listes ACL employant des séquences d'entrées, la règle de recherche est définie de telle sorte que la première entrée qualificative termine la recherche. L'ordonnancement de telles listes ACL est donc important, car il permet l'expression de politiques dans lesquelles des initiateurs individuels peuvent se voir spécifiquement dénier l'accès même si pour une autre correspondance plus générale, par exemple, pour les initiateurs d'un groupe, les initiateurs ont le droit d'accès.

8.2.4.2 Listes ACL avec des initiateurs groupés

L'information de liste ACL peut être structurée pour refléter, pour un ensemble d'initiateurs, le groupement de droits d'accès similaires. De plus, lorsque les cibles sont elles-mêmes groupées, les listes ACL peuvent être associées à des groupes de cibles. Une hiérarchie de listes ACL peut être utilisée avec des listes ACL de haut niveau, fournissant sur un large groupe de cibles une information de contrôle d'accès grossier, sur lesquelles des listes ACL pour des sous-groupes de cibles peuvent être superposées.

8.2.4.3 Listes ACL avec qualificatif de cible

Cette extension est particulièrement importante lorsqu'une liste de contrôle d'accès n'est pas colocalisée avec une cible spécifique. Une cible doit être spécifiée dans chaque entrée de la liste ACL. Les entrées de la liste ACL sont structurées en trois parties:

- qualificatif d'initiateur;
- qualificatif de demande d'accès;
- qualificatif de cible.

L'algorithme de correspondance compare l'information ACI d'initiateur, l'information ACI de demande d'accès, et de cible avec chaque qualificatif d'initiateur, qualificatif d'action, entrée de qualificatif de cible de la liste de contrôle d'accès.

8.2.4.4 Listes ACL avec cibles groupées

Cette extension met en jeu le partage d'une seule liste ACL entre plusieurs cibles afin que les décisions déterminées par une liste ACL fassent référence à plusieurs cibles. Lorsqu'une seule cible est sujette au critère de décision de plusieurs listes ACL, le mécanisme de politique de contrôle d'accès doit spécifier la règle requise pour combiner les décisions résultantes.

8.2.4.5 Listes ACL avec qualificatif de contexte

Cette extension met en jeu l'utilisation de l'information de contexte. Les entrées de listes ACL sont structurées en trois parties:

- qualificatif d'initiateur;
- qualificatif de demande d'accès;
- qualificatif de contexte.

Le qualificatif de contexte est un qualificatif additionnel qui décrit les restrictions de contexte pour cette entrée. L'algorithme de correspondance compare l'information ACI d'initiateur, la demande d'accès et l'information de contexte avec chaque qualificatif d'initiateur, qualificatif de demande d'accès, entrée de qualificatif de contexte de la liste de contrôle d'accès.

8.2.4.6 Listes ACL avec correspondance partielle

Dans certaines réalisations, dans lesquelles des parties de l'identité ou d'autres informations ACI doivent être comparées avec le qualificatif d'initiateur, des qualificatifs de correspondance partielle, sont mis en œuvre. Par exemple, si un initiateur a un nom qui est construit par une séquence de noms de composants (tels que pays, organisation, unité organisationnelle, nom-personnel) la liste ACL peut être construite pour reconnaître un ou plusieurs composants pouvant être vus comme des entités d'un groupe.

8.2.4.7 Listes ACL sans qualificatif de demande d'accès

Dans cette variante de la structure de liste d'ACL, les ensembles ou les séquences ne contiennent pas de qualificatifs de demande d'accès. Aucun qualificatif de demande d'accès n'est mis en jeu dans la fonctionnalité Décider l'accès. Si un accès d'un initiateur est autorisé, il est autorisé pour tous les accès.

8.3 Structure de capacité

8.3.1 Caractéristiques élémentaires

Les caractéristiques élémentaires de la structure de capacité sont:

a) le contrôle d'accès est géré en tant qu'information ACI attachée à l'initiateur (une capacité) définissant un ensemble d'opérations autorisées sur un ensemble identifié de cibles;

b) cette structure de contrôle d'accès est pratique lorsqu'il y a peu de cibles;

c) cette structure de contrôle d'accès n'est pas pratique pour révoquer l'accès à une cible au niveau de celle-ci à moins qu'il ne soit possible d'identifier individuellement les capacités une fois qu'elles sont accordées à l'initiateur; mais cette structure est pratique pour une autorité SDA d'initiateur désirant révoquer les droits d'accès de cet initiateur;

d) cette structure de contrôle d'accès est pratique lorsque la gestion d'un contrôle d'accès est réalisée au niveau de l'initiateur;

e) les capacités sont pratiques lorsqu'il y a «plusieurs» utilisateurs ou «plusieurs» groupes d'utilisateurs accédant à «quelques» cibles et lorsque la cible et les utilisateurs sont dans différents domaines de sécurité.

NOTE – L'utilisation de mots de passe pour le contrôle d'accès est proche mais distincte des capacités. Les caractéristiques élémentaires des mots de passe sont:

– le contrôle d'accès est basé sur l'information ACI partagée entre l'initiateur et la cible;

– le contrôle d'accès dépend de la confidentialité de l'information ACI maintenue par l'initiateur et la cible ainsi que de la confidentialité durant le transfert (il est souvent difficile de maintenir la confidentialité des mots de passe);

– les changements de mots de passe peuvent être difficiles si plusieurs initiateurs partagent le même mot de passe.

8.3.2 Information ACI

8.3.2.1 Information ACI attachée à l'initiateur

L'information ACI attachée à l'initiateur est un ensemble de capacités.

Une capacité a deux principaux composants:

a) le nom de la cible ou de l'ensemble des cibles;

b) la liste des opérations autorisées sur une cible.

Les capacités peuvent être transportées par un certificat de contrôle d'accès signé ou scellé sous l'autorité de l'autorité SDA.

8.3.2.2 Information ACI attachée à la cible

L'information ACI attachée à la cible est un ensemble d'entrées. Chaque entrée a deux composants:

a) l'identité de l'autorité SDA;

b) les opérations que l'autorité SDA peut autoriser.

8.3.3 Mécanismes de support

L'initiateur obtient un certificat de contrôle d'accès ou un jeton de contrôle d'accès en utilisant la fonctionnalité Acquérir l'information ACI attachée à l'initiateur qui est alors attachée à une demande de contrôle d'accès par l'initiateur en utilisant la fonctionnalité Générer l'information ACI attachée à la demande d'accès et, finalement, est vérifiée par la fonction ADF en utilisant la fonctionnalité Vérifier l'information ACI attachée et Dériver l'information ADI.

L'information ADI d'initiateur (par exemple, le contenu de la capacité), le nom de l'opération et l'information ADI de cible sont les paramètres du dispositif Décider l'accès. L'information ADI de cible est contrôlée pour vérifier qu'elle est un des noms de cibles et l'opération est contrôlée pour vérifier qu'elle fait partie de celles citées dans la capacité. L'accès est autorisé si les deux contrôles réussissent.

La fonctionnalité Décider l'accès indiquera que l'accès devrait être dénié si:

a) la capacité présentée n'est pas reconnue comme une capacité valide;

b) l'accès à la cible est affirmé sur les opérations autorisées improprement par l'autorité SDA (par exemple, l'autorité SDA n'est pas autorisée à permettre ces opérations);

c) l'opération dérivée de la demande d'accès ne correspond pas à la capacité.

8.3.4 Variantes de cette structure – Capacités sans opérations spécifiques

Dans cette variante de la structure de capacité, aucun ensemble d'opérations autorisées n'est contenu dans la capacité et aucun nom d'opération n'est fourni au dispositif Décider l'accès. Si un accès d'un initiateur est autorisé, il est autorisé pour toutes les opérations.

8.4 Structure fondée sur l'étiquette

8.4.1 Caractéristiques élémentaires

Les caractéristiques élémentaires de la structure fondée sur l'étiquette sont:

a) cette structure utilise des étiquettes de sécurité pouvant être affectées aux initiateurs et aux cibles, et les données échangées entre systèmes;

b) cette structure est plus pratique lorsqu'il y a plusieurs initiateurs accédant à plusieurs cibles et seulement un niveau de finesse grossier est nécessaire pour le contrôle d'accès;

c) étant donné certaines restrictions de politique, cette structure peut être utilisée pour contrôler le flux de données au sein d'un domaine de sécurité. Les étiquettes de sécurité peuvent également s'avérer pratiques pour fournir le contrôle d'accès entre domaines de sécurité;

d) les opérations autorisées ne sont pas explicitement incluses dans l'information ACI attachée à l'initiateur ou attachée à la cible, mais sont définies dans la politique de sécurité.

NOTES

1 Les étiquettes ne sont pas nécessairement de simples structures.

2 Lorsqu'un initiateur est un utilisateur humain (ou lorsqu'un processus d'initiateur représente un utilisateur humain), l'étiquette attachée à l'initiateur est souvent appelée une autorisation. Dans ces cas, l'étiquette attachée à la cible est appelée une classification.

8.4.2 Information ACI

8.4.2.1 L'information ACI attachée à l'initiateur

L'information ACI attachée à l'initiateur est une étiquette de sécurité.

8.4.2.2 Information ACI attaché à la cible

L'information ACI attachée à la cible est une étiquette de sécurité.

NOTE – Les représentations de l'information ACI attachée à l'initiateur et de l'information ACI attachée à la cible sont habituellement structurées de façon à faciliter leur comparaison, cependant, la même représentation n'a pas besoin d'être utilisée pour les deux informations. La traduction de représentation d'information de sécurité est présentée dans la Rec. UIT-T X.810 | ISO/CEI 10181-1.

8.4.2.3 Information ACI attachée à l'opérande

Les opérandes d'une demande d'accès peuvent avoir des étiquettes attachées. Les opérandes étiquetés constituent un cas particulier de données étiquetées.

Deux propriétés de sécurité de données étiquetées doivent être garanties: l'intégrité de l'attachement de l'étiquette aux données, et le droit de l'initiateur à créer des données avec cette étiquette.

Etant donné certaines restrictions de politique, l'étiquetage de la sécurité peut être utilisé pour fournir le contrôle d'accès général aux données au sein d'un domaine de sécurité ou entre domaines de sécurité.

Des exemples de données étiquetées comprennent:

– documents;

– messages;

– unités de données sans connexion;

– fichiers en transfert.

8.4.3 Mécanismes de support

Quatre mécanismes peuvent être utilisés pour obtenir l'information ACI attachée à l'initiateur ou l'information ACI attachée à l'opérande utilisée dans la fonctionnalité Décider l'accès:

a) *en utilisant des certificats de contrôle d'accès ou des jetons de sécurité*

Voir 8.2.3.

b) *en utilisant l'authentification et la consultation*

La fonction ADF obtient l'identité authentifiée de l'initiateur et l'utilise pour consulter son autorisation.

c) *en utilisant un canal étiqueté*

L'autorisation de l'initiateur ou l'étiquette des données peut être déduite de l'étiquette du canal utilisé pour transporter la demande d'accès. L'intégrité de l'attachement d'une étiquette à un canal peut être garantie par l'utilisation d'un service d'intégrité. La garantie que le canal a été «correctement» affecté peut être réalisée en faisant confiance au fournisseur du service de communications pour la vérifier. De façon similaire, la garantie qu'une entité cible est autorisée à accepter un canal peut être obtenue en faisant confiance au fournisseur du service de communications pour vérifier l'autorisation avant que le canal soit établi.

d) *en utilisant des données étiquetées*

L'autorisation de l'initiateur peut être déduite des étiquettes des opérandes de la demande d'accès. L'intégrité de l'attachement d'une étiquette à des données peut être assurée soit par l'intégrité du canal sous-jacent soit par le biais de l'utilisation d'un code de vérification d'intégrité ou d'une signature numérique, produite par l'autorité SDA, sur les données et l'étiquette de sécurité.

Une étiquette de sécurité peut être utilisée comme information ACI de cible pour protéger une cible. Des règles d'accès définissent les permissions d'accès (opérations) accordées en fonction de l'étiquette de sécurité de l'initiateur et de l'étiquette de sécurité affectée à la cible.

Si la politique de sécurité nécessite que les informations ACI conservées dans l'étiquette de sécurité soient utilisées pour l'information ACI de cible, alors le flux complet de données entrant et sortant de cette cible peut être contrôlé. Ainsi, le flux complet de données entrant et sortant des cibles peut être analysé pour des domaines de sécurité appliquant la même politique de sécurité.

Des cibles peuvent être créées au sein d'autres cibles. L'étiquette de sécurité de la cible contenante limite les étiquettes de sécurité pouvant être affectées à la cible contenue dans le cadre des règles pour la politique de sécurité appropriée.

Des exemples de cibles auxquelles des étiquettes peuvent être appliquées comprennent:

- entités N OSI;
- entrées du service d'annuaire;
- fichiers gardés dans une réserve de fichiers;
- entrées de base de données.

8.4.4 Voies étiquetées comme cibles

Le créateur du canal (par exemple l'autorité SDA) affecte une étiquette de sécurité à un canal. Pour utiliser le canal, une information ACI de l'initiateur et l'étiquette de sécurité affectée au canal constituent l'entrée de la fonctionnalité Décider l'accès. C'est-à-dire que le canal est considéré comme une cible. Les étiquettes des données transportées dans ce canal doivent être cohérentes avec l'étiquette du canal.

L'étiquette affectée au canal peut également être utilisée pour contrôler la route du canal. En termes OSI, les entités de couche N et les systèmes de relais accèdent aux connexions de couche N – 1 ou aux unités de données sans connexion, ainsi les entités de couche N doivent satisfaire les règles d'accès pour les connexions de couche N – 1 ou des unités de données sans connexion.

Des exemples de voies étiquetées comprennent:

- associations A;
- connexions de couche n OSI;
- canal interprocessus.

8.5 Structure fondée sur le contexte

8.5.1 Caractéristiques élémentaires

Dans certains cas, la fonction ADF peut avoir besoin d'informations de contexte pour interpréter l'information ADI ou les règles de politique de sécurité. Les caractéristiques élémentaires de la structure fondée sur le contexte sont:

a) le contrôle d'accès est géré en termes d'information ACI attachée à l'initiateur ou d'information ACI attachée à la cible ou de façon indépendante comme information obtenue par la fonction ADF;

b) cette structure est pratique pour imposer des règles applicables à tous les initiateurs.

8.5.2 Information ACI

8.5.2.1 Listes de contrôle de contexte

Les listes de contrôle de contexte sont des ensembles ou des séquences d'entrées. Chaque entrée comprend deux champs:

a) *qualificatif de contexte*

Le qualificatif de contexte est une séquence de conditions de contexte (par exemple, l'heure, la route, le lieu) sur laquelle une opération de qualificatif est appliquée. Chaque condition de contexte est associée individuellement à une assertion vraie ou fausse.

b) *qualificatif d'opération*

Cela décrit les opérations autorisées pour le qualificatif de contexte associé.

8.5.2.2 Information de contexte

Cette information est obtenue à partir du contexte où la demande d'accès est réalisée.

Le contexte dépend de l'environnement dans lequel la demande d'accès est reçue par la fonction ADF. Il y a différentes façons d'obtenir l'information de contexte, par exemple à partir d'une interface de service en couche sous-jacente ou d'une interface locale de gestion.

8.5.3 Mécanismes de support

La fonction ADF utilise la fonctionnalité Obtenir l'information de contexte pour obtenir l'information de contexte. L'information de contexte et la demande d'accès constituent les entrées de la fonctionnalité Décider l'accès. L'opération demandée, dérivée à partir de la demande d'accès, et l'information de contexte fournie sont respectivement comparées au qualificatif d'opération et au qualificatif de contexte, pour déterminer si l'accès est autorisé ou dénié.

8.5.4 Variantes de cette structure

Dans certaines listes de contrôle de contexte employant des séquences d'entrées, la règle de recherche est telle que la première entrée qualificative termine la recherche. Pour chaque entrée la règle est que l'accès est dénié si l'information de contexte n'est pas conforme à toutes les conditions de contexte. Par exemple, cela autoriserait des politiques comme celles autorisant une opération particulière seulement à partir de certains endroits durant une certaine période de temps, mais n'utilisant pas une route particulière.

9 Interaction avec d'autres services et mécanismes de sécurité

Cet article décrit la façon dont d'autres services et mécanismes de sécurité peuvent être utilisés pour mettre en œuvre le contrôle d'accès. L'utilisation du contrôle d'accès pour mettre en œuvre d'autres services de sécurité n'est pas décrite ici.

9.1 Authentification

La nature des services de contrôle d'accès et d'authentification est quelquefois mal comprise. Bien qu'il y ait certains points communs et certaines relations, les services ne sont pas les mêmes. Certaines structures de contrôle d'accès (par exemple, les listes ACL) s'appuient sur des identités et, donc, nécessitent l'authentification pour garantir l'identité. Une authentification couronnée de succès peut conduire à l'obtention de certaines informations ACI par l'initiateur. Il est à noter que dans certains systèmes la fonctionnalité Vérifier pour l'authentification et la fonction ADF sont colocalisées. Dans ces cas, un échange d'authentification est le seul protocole visible. Dans des systèmes distribués, ces fonctions ne sont pas nécessairement colocalisées et une information ACI d'initiateur distincte peut être utilisée. Une identité est alors simplement considérée en tant que partie de l'information ACI de l'initiateur.

La relation entre authentification et contrôle d'accès peut être spécifiée par la politique de contrôle d'accès. Par exemple, si l'initiateur est authentifié par un mécanisme moins sûr, la politique de contrôle d'accès peut imposer que certaines opérations (par exemple, modifier) ne puissent pas être réalisées sur la cible. D'un autre côté, si l'initiateur est authentifié par un mécanisme plus sûr, ces opérations seraient permises.

9.2 Intégrité des données

Le service d'intégrité des données peut être utilisé pour assurer l'intégrité des entrées et des sorties au sein de et entre les composants de contrôle d'accès, par exemple, pour éviter la modification des capacités, des listes ACL et de l'information de contexte stockée ou transférée.

9.3 Confidentialité des données

Le service de confidentialité des données peut être requis dans le cadre de certaines politiques de sécurité pour établir la confidentialité de certaines entrées et sorties dans et entre composants de contrôle d'accès, par exemple, pour se protéger de l'accumulation d'informations sensibles.

9.4 Audit

L'information ACI peut être utilisée pour faire l'audit des demandes d'accès d'un initiateur particulier. Il peut être nécessaire de rassembler plusieurs journaux d'audit de sécurité pour être en mesure d'identifier les demandes d'accès qui ont été effectuées et leurs initiateurs.

Une politique d'audit de sécurité peut nécessiter l'enregistrement de certaines ou de toutes les tentatives d'accès. Ainsi, la disponibilité d'un mécanisme d'enregistrement sûr peut être requise pour un mécanisme de contrôle d'accès. Une politique d'audit de sécurité peut également nécessiter des informations sur le fonctionnement du mécanisme de contrôle d'accès à enregistrer (par exemple, les circonstances dans lesquelles les accès ont été déniés). Une politique de contrôle d'accès peut requérir qu'aucun accès non vérifié n'ait lieu, dans ce cas le mécanisme de contrôle d'accès dépendra fonctionnellement du service d'enregistrement fiable.

Dans les cas où l'imputabilité de l'initiateur est nécessaire, l'initiateur est toujours sujet à l'authentification avant un accès. Il est important de comprendre que l'authentification et le contrôle d'accès, bien que souvent fortement liés, ne sont pas toujours réalisés par des fonctions sous le contrôle des mêmes autorités, et que les fonctions n'ont pas besoin d'être colocalisées. L'information utilisée pour l'authentification peut être nécessaire pour obtenir l'information ACI attachée à l'initiateur (voir 8.5 et 9.1 pour une présentation plus détaillée).

L'accès anonyme avec imputabilité peut être fourni de la façon suivante:

- l'initiateur obtient de l'autorité SDA l'information ACI incluant un identificateur d'audit associé. L'acquisition de l'information ACI est enregistrée: l'identité de l'initiateur et l'identificateur d'audit sont conservés dans le journal d'audit du domaine de sécurité émettant l'information ACI;
- l'initiateur utilise l'information ACI attachée à l'initiateur pour accéder à la cible. La fonction ADF du domaine de sécurité de la cible qui reçoit l'information ACI attachée à l'initiateur stocke l'identificateur d'audit et la demande d'accès dans son journal d'audit;
- une autorité SDA ayant accès à l'information d'audit à la fois à partir du domaine de sécurité de la cible et à partir du domaine de sécurité émettant l'information ACI attachée à l'initiateur peut, en utilisant l'identificateur d'audit, identifier l'initiateur. Par ce moyen, l'initiateur peut être tenu responsable pour son accès.

S'il y a un conflit entre le désir d'anonymat de l'initiateur et les besoins de connaissance, par le domaine de sécurité de la cible, de l'identité de l'initiateur, l'accès peut être rejeté; la décision dépend de la politique de contrôle d'accès du domaine de sécurité de la cible.

9.5 Autres services liés à l'accès

Le contrôle d'accès n'est pas le seul service dont la mise en œuvre est réalisée au moment où une demande d'accès est effectuée. L'audit (ci-dessus), l'imputabilité, et l'accusation sont d'autres services liés à la sécurité qui fonctionnent au moment d'une demande d'accès:

- un service d'audit enregistre des informations arbitraires sur la demande d'accès;
- un service d'imputabilité vérifie spécifiquement le nom ou les noms des entités formellement responsables du déclenchement de la demande d'accès;
- un service de comptabilité garantit qu'un compte est débité d'un montant approprié pour l'utilisation de la ressource accédée.

L'information requise, au moment d'une demande d'accès, pour réaliser chacun de ces services est logiquement différente. Les informations ADI fournies par le contrôle d'accès, le nom du compte pour la comptabilité, et l'identification de l'entité responsable pour l'imputabilité, peuvent être toutes différentes. Cependant, dans certaines réalisations, il est nécessaire d'utiliser la même information (par exemple, l'identité du contrôle d'accès) pour chacune de celles-ci. Cela peut causer une confusion, spécialement en présence des demandes d'accès envoyées. Il est préférable de garder les différents types d'information distincts.

Annexe A

Echange de certificats de contrôle d'accès entre composants

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

A.1 Introduction

Le but de cette annexe est de donner un exemple pratique de la façon dont les certificats de contrôle d'accès peuvent être envoyés entre composants lorsque certains composants agissent en même temps comme cibles et initiateurs, et pour établir les exigences générales pour passer dans un accès chaîné les multiples certificats de contrôle d'accès entre différents composants.

A.2 Envoi des certificats de contrôle d'accès

L'aperçu des cadres de sécurité décrit plusieurs mécanismes permettant à une entité ayant le droit d'utiliser un certificat de sécurité de transférer ce droit à d'autres entités. Dans les cas où une entité B fait des demandes d'accès pour le compte d'une autre entité A, ces mécanismes peuvent être utilisés pour transférer le droit d'utiliser un certificat de contrôle d'accès de A vers B.

A.3 Envoi de multiples certificats de contrôle d'accès

Dans certains cas, il peut être nécessaire d'utiliser plusieurs certificats de contrôle d'accès pour effectuer une interaction complexe. Ce besoin est d'abord illustré au moyen d'un exemple. Cela donne une vue des origines et des usages des différents certificats de contrôle d'accès qui pourraient être requis. Trois classes de certificats de contrôle d'accès sont identifiées, chacun de ceux-ci a des caractéristiques différentes. L'exemple est ensuite étendu pour donner une vue plus générale.

A.3.1 Exemple

Supposons que l'application A2 soit accédée par l'application A1 utilisée par l'utilisateur U. Chaque demande d'accès est de A1 vers A2. Cependant, A2 peut utiliser les services d'une autre application A3 pour répondre à la demande d'accès qui, à son tour, pourrait avoir besoin des services d'une application A4, comme cela est illustré sur la Figure A.1.

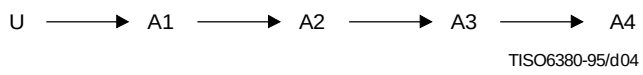

Figure A.1 – Envoi de multiples certificats de contrôle d'accès

Considérons d'abord la relation entre A1 et A2 et les certificats de contrôle d'accès qu'il peut être nécessaire d'associer à une demande d'accès de A1 à A2. Deux certificats de contrôle d'accès peuvent être nécessaires: pour l'utilisateur U et pour l'application A1.

Il y a trois classes de contrôle de certificats de contrôle d'accès pouvant être nécessaires à la fois pour l'utilisateur U et pour l'application A1:

- les certificats de contrôle d'accès requis pour accéder à A2 valides pour toutes les opérations;
- les certificats de contrôle d'accès requis pour accéder à A2 valides pour un ensemble défini d'opérations;
- les certificats de contrôle d'accès requis pour accéder à A2 valides pour une seule opération.

En principe, chaque certificat de contrôle d'accès peut être obtenu auprès d'une autorité SDA différente.

Les certificats de contrôle d'accès valides pour toutes les opérations sont transportés au début d'une connexion ou d'une association.

Lorsque des certificats de contrôle d'accès définissent un ensemble valide d'opérations, ils demeurent inchangés jusqu'à ce que d'autres certificats de contrôle d'accès de cette classe soient transportés.

Les certificats de contrôle d'accès valides pour une seule opération sont attachés à la seule opération.

A.3.2 Généralisation

Considérons ensuite les relations entre A2 et A3 et les certificats de contrôle d'accès qu'il peut être nécessaire d'associer à un accès demandé par A2 sur A3. Ces certificats de contrôle d'accès peuvent être nécessaires: pour l'utilisateur U, pour l'application A1, et pour l'application A2.

Les certificats de contrôle d'accès pour l'utilisateur U et l'application A1 destinés à être utilisés au niveau de A2 peuvent ou non être acceptables pour une utilisation au niveau de A3. S'ils sont acceptables, chacun de ces certificats peut faire partie de n'importe laquelle des trois classes décrites ci-dessus. S'ils ne sont pas acceptables, alors l'utilisateur U ou l'application A1 (ou les deux), lorsqu'ils effectuent une demande d'accès sur A2, doivent fournir un certificat de contrôle d'accès additionnel, destiné à être utilisé au niveau A3, pouvant, à nouveau, faire partie de n'importe laquelle des trois classes décrites ci-dessus.

Cette structure peut être généralisée pour la relation entre A3 et A4, avec de possibles certificats additionnels requis pour U, A1 et A2.

A.3.3 Simplifications

Habituellement seul le certificat de contrôle d'accès de l'utilisateur U ou le certificat de contrôle d'accès de l'application A1 est nécessaire. Les certificats de contrôle d'accès valides seulement pour une opération unique ne sont que rarement utilisés. Un certificat de contrôle d'accès de U destiné à être utilisé en A2 peut être envoyé par A1 même s'il n'est pas utilisé en A1.

Annexe B

Contrôle d'accès dans le modèle de référence OSI

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

NOTE – Ce texte est basé sur la Rec. X.800 du CCITT | ISO 7498-2.

B.1 Généralités

Le contrôle d'accès peut être utilisé au moment de l'établissement de la phase de transfert des données d'une connexion ou à des instants de la connexion. Ce service est disponible à la fois pour les protocoles orientés connexion et les protocoles sans connexion.

B.2 Utilisation du contrôle d'accès dans les couches OSI

Le contrôle d'accès a seulement du sens pour les couches OSI suivantes:

– couche réseau (couche 3);

– couche transport (couche 4);

– couche application (couche 7).

B.2.1 Utilisation du contrôle d'accès pour la couche réseau

Lorsqu'il est utilisé pour la couche réseau le contrôle d'accès autorise le contrôle d'accès de et/ou vers les nœuds de réseau, les nœuds de sous-réseau ou les relais. Le contrôle d'accès dans la couche réseau peut avoir plusieurs objectifs. Par exemple, il permet à un système d'extrémité de contrôler l'établissement de connexions réseau et de rejeter les appels qui ne sont pas souhaités. Il permet à un ou plusieurs sous-réseaux de contrôler l'utilisation des ressources de la couche réseau. Dans certains cas, ce dernier but est lié à la comptabilité de l'utilisation du réseau.

Les mécanismes de contrôle d'accès utilisés par la couche réseau sont situés au sein de la même couche.

B.2.2 Utilisation du contrôle d'accès pour la couche transport

Lorsqu'il est utilisé pour la couche transport, le contrôle d'accès autorise le contrôle d'accès de et/ou vers les entités session. Différentes applications de mises en œuvre par le même système d'extrémité ne peuvent pas être contrôlées séparément si elles partagent une connexion de transport.

Les mécanismes utilisés par la couche transport sont situés au sein de la même couche.

B.2.3 Utilisation du contrôle d'accès pour la couche application

Se reporter à l'interconnexion des systèmes ouverts – Modèle de sécurité des couches hautes (ISO 10745).

Annexe C

Non-unicité des identités de contrôle d'accès

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

Deux exemples sont utilisés pour démontrer les problèmes potentiels dans l'affectation et l'utilisation des identités de contrôle d'accès:

- si un utilisateur nommé Pierre Durand, supposé être un nom très courant, se voit affecter, en tant qu'identité individuelle de contrôle d'accès, la chaîne de caractère «Pierre Durand» dans un domaine de sécurité particulier, alors la même chaîne de caractère peut être placée dans un attribut de contrôle afin d'accorder certains accès autorisés pour cet utilisateur. Pierre Durand peut ensuite quitter ce domaine de sécurité et une autre personne également appelée Pierre Durand peut plus tard entrer dans le même domaine de sécurité et se voir affecter l'identité individuelle de contrôle d'accès «Pierre Durand»Si la chaîne de caractère «Pierre Durand» est encore dans un attribut de contrôle, alors le nouveau Pierre Durand sera en mesure de réaliser les accès autorisés pour l'ancien Pierre Durand;

- si une cible se voit affecter, en tant qu'identité de contrôle d'accès, une chaîne de caractère, la même chaîne de caractère peut ensuite être utilisée dans un attribut de privilège afin d'accorder certains accès autorisés à un utilisateur. Plus tard, la cible peut être enlevée de ce domaine de sécurité et, encore plus tard, une autre cible peut être créée sous la même identité de contrôle d'accès. Si l'attribut de privilège donné à l'utilisateur n'a pas été modifié, il apparaîtra valide pour accéder à la nouvelle cible.

Les identités de contrôle d'accès sont supposées être uniques dans un domaine de sécurité. Cependant, une identité peut être valide seulement durant des intervalles de temps spécifiques ou, peut-être, effectivement tout le temps. Lorsqu'une identité est valable seulement durant des intervalles de temps spécifiques, un type d'attribut donné avec cette identité de contrôle d'accès comme une valeur d'attribut a, à tout instant, une signification particulière. Cependant, si des précautions insuffisantes sont prises, le même type d'attribut et la même valeur d'attribut pourraient être réutilisés. S'il existe encore une instance d'un type d'attribut précédent ou d'une valeur précédente d'attribut, alors une brèche peut survenir dans la sécurité.

Il y a deux façons de résoudre ce problème. Avant de définir un nouveau type d'attribut de contrôle d'accès ou de valeur d'attribut de contrôle d'accès, l'autorité SDA doit garantir que ce type d'attribut de contrôle d'accès ou cette valeur d'attribut de contrôle d'accès:

- n'est pas actuellement affecté;

- n'a précédemment jamais été utilisé.

Dans le premier cas, l'autorité SDA a besoin d'être sûre que chaque fois qu'un type d'attribut de contrôle d'accès ou qu'une valeur d'attribut de contrôle d'accès est enlevé, aucun initiateur ou cible ne possède encore le type d'attribut de contrôle d'accès ou la valeur d'attribut de contrôle d'accès donné. Lorsque cela n'est pas possible, alors une période de validité (implicite ou explicite) pour chaque type d'attribut de contrôle d'accès ou valeur d'attribut de contrôle d'accès doit être définie. Au sein de cette période de validité, il est nécessaire de garder trace de tous les types d'attributs de contrôle d'accès ou de toutes les valeurs d'attributs de contrôle d'accès enlevés.

Dans le second cas, une identité de contrôle d'accès unique (également appelée identificateur permanent) qui soit une valeur affectée seulement une fois et qui ne puisse jamais être réutilisée, doit être définie.

Annexe D

Distribution des composants de contrôle d'accès

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

Les fonctions élémentaires de contrôle d'accès, AEF et ADF, peuvent être composées d'un ou plusieurs composants qui, lorsqu'ils sont combinés, réalisent les fonctions AEF ou ADF (composants de fonction AEF-composants de fonction AEC et ADF-ADC). Dans le paragraphe 5.2 les fonctions sont présentées indépendamment des considérations de localisation des composants, des communications entre eux, ou de leur possible distribution. Les problèmes liés au contrôle d'accès entre composants sous le contrôle de différentes autorités SDA sont présentés au 5.4.

D.1 Aspects considérés

Les intérêts particuliers dans la présentation suivante sont:

- le nombre et la localisation des composants AEC et ADC;
- les interactions entre les initiateurs, les composants AEC, les composants ADC, et les cibles.

Dans tout domaine de sécurité, un ou plusieurs composants AEC seront interposés entre chaque initiateur-instance cible afin qu'un initiateur puisse agir sur une cible seulement par le biais de composants AEC. Il y a plusieurs mises en œuvre physiques possibles pour les composants AEC et ADC. A savoir:

- une fonction AEF peut être distribuée de différentes façons; celles-ci sont présentées en D.3 et illustrées sur les Figures D.1, D.2 et D.3;
- un composant ADC peut on non être colocalisé (fortement couplé) avec un composant AEC;
- un composant ADC peut servir un seul composant AEC ou il peut servir plusieurs composants AEC;
- un composant AEC peut utiliser un seul composant ADC ou plusieurs composants ADC.

Il y a plusieurs ordonnancements possibles pour les communications entre les composants présents.

D.2 Localisation des composants AEC et ADC

Les composants AEC peuvent être des constituants (internes) d'un système d'extrémité ou interposés (externes) entre le système d'extrémité et le réseau utilisé pour communiquer avec d'autres systèmes d'extrémité comme cela est illustré sur la Figure D.1. Certains systèmes réels peuvent employer à la fois des composants constitutifs ou interposés pour répondre aux différents aspects du contrôle de sécurité. Les avantages et les désavantages de composants AEC internes et externes sont liés à la politique, aux problèmes de confiance des mises en œuvre, et à d'autres considérations non couvertes ici.

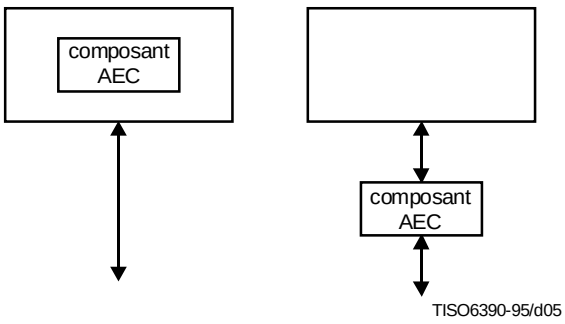

Figure D.1 – Mises en œuvre interne et externe de fonction AEF

De façon similaire, les composants ADC peuvent être internes ou externes aux systèmes d'extrémité comme cela est illustré sur la Figure D.2. Pour les composants ADC servant à un seul composant AEC externe, il est probable, mais non nécessaire, que le composant ADC soit également externe. Pour les composants ADC servant plusieurs composants AEC dans différents systèmes d'extrémité, le composant ADC sera habituellement externe. Comme indiqué précédemment, un système d'extrémité pourrait employer de multiples composants AEC pour différents aspects du contrôle de sécurité. Dans de tels cas, un seul composant ADC interne ou externe pourrait servir des composants AEC ou de multiples composants ADC spécialisés pourraient être utilisés. La colocalisation (couplage fort) d'un composant AEC et d'un composant ADC peut présenter des avantages en termes d'efficacité et de délais (en réduisant le retard).

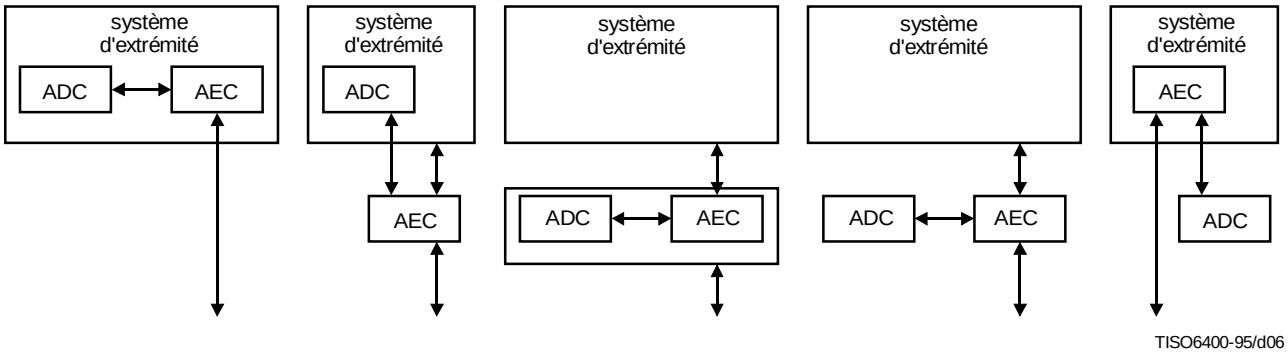

Figure D.2 – Mises en œuvre des fonctions AEF/ADF

D.3 Interactions entre composants de contrôle d'accès

La fonction ADF peut être mise en œuvre par un ou plusieurs composants ADF et la fonction AEF peut être mise en œuvre par un ou plusieurs composants de fonction AEF. Les relations entre les composants de contrôle d'accès sont explorées dans cette sous-clause et sont illustrées sur la Figure D.3. Les relations décrites ici s'appliquent seulement à un initiateur unique et à une cible unique. D'autres exemples pourraient inclure un composant AEC utilisant plusieurs composants ADC.

Dans (a), l'initiateur (I) présente sa demande d'accès directement au composant AEC d'initiateur qui demande approbation au composant ADC. Si l'accès est approuvé, le composant AEC notifie la demande à la cible (T).

Dans (b), l'initiateur présente la demande d'accès directement au composant AEC de cible qui, à son tour, la présente au composant ADC pour approbation. Si l'accès est approuvé, le composant AEC notifie la demande à la cible.

Il existe une corrélation entre la fonctionnalité et la localisation dans (a) et (b). Le composant AEC réalise le contrôle d'accès entrant ou sortant ou les deux, et peut donc être appelé composant AEC initiateur, cible ou interposé.

Dans (c), l'initiateur présente la demande d'accès au composant AEC interposé qui, à son tour, la présente au composant ADC pour approbation. Si l'accès est approuvé, le composant AEC notifie la demande à la cible.

Dans (d), l'interaction est une composition de (a) et (b) avec le même composant ADC approuvant la demande d'accès pour les composants AEC d'initiateur et de cible. L'initiateur présente sa demande d'accès au composant AEC d'initiateur qui demande approbation au composant ADC. Si l'accès est approuvé, le composant AEC d'initiateur présente la demande d'accès au composant AEC de cible qui, à son tour, la présente au composant AEC pour approbation. Si l'accès est approuvé, le composant AEC de cible notifie la demande à la cible.

Dans (e) et (f), les composants AEC séparés appliquent le contrôle d'accès sortant et entrant. Dans (e), l'interaction est similaire à (c) à l'exception du fait que les deux composants AEC doivent approuver l'accès demandé. Dans (f), l'interaction est une composition de (a) et (b), avec des composants AEC séparés.

La présentation précédente a été par nature simpliste. Cependant, des interactions plus complexes entre l'initiateur, la cible et les composants AEC sont considérées possibles, pour inclure le séquencement, l'emboîtement et les entrées récursives.

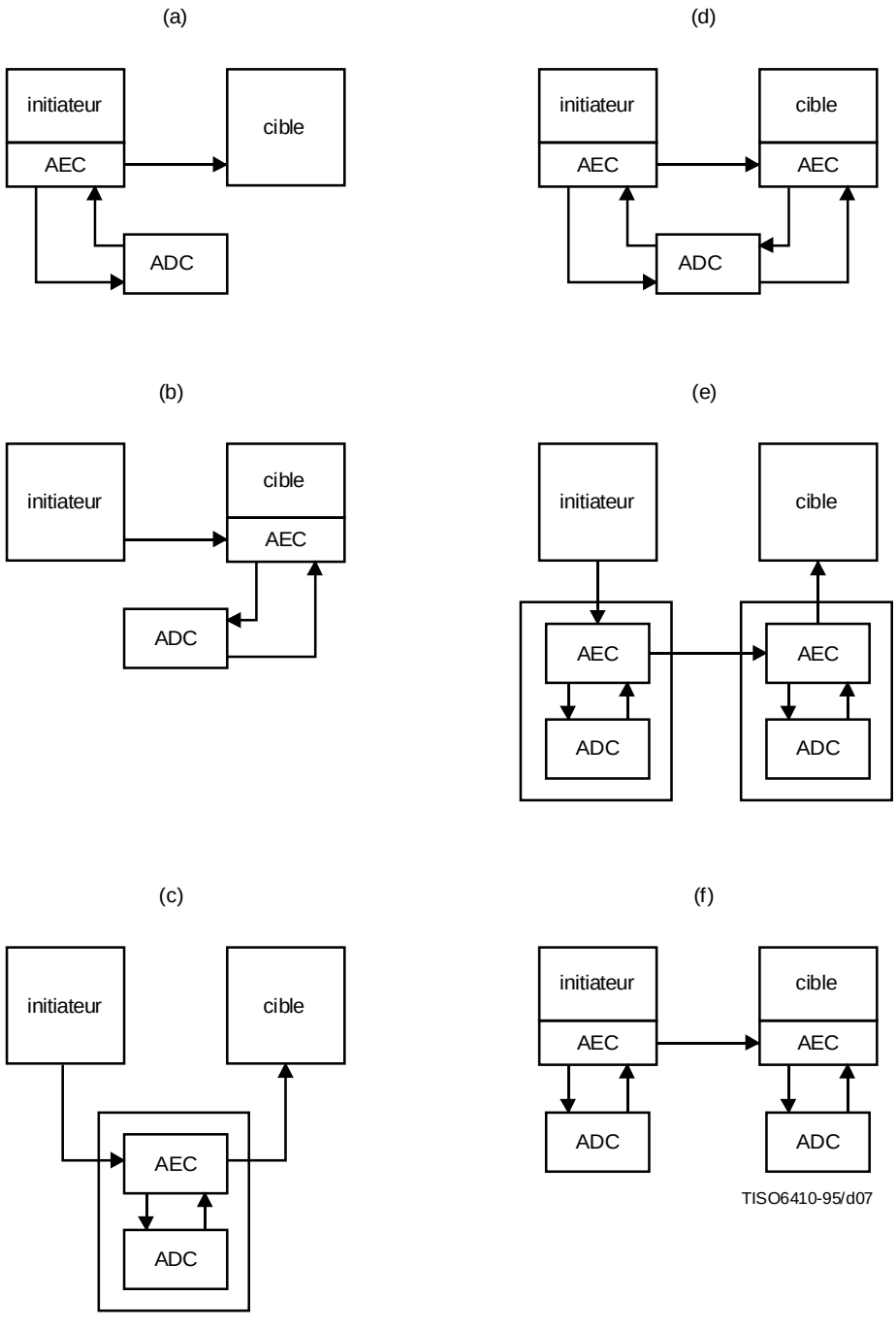

Figure D.3 – Relations des composants

Annexe E

Politiques fondées sur les règles versus politiques fondées sur l'identité

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

Les politiques de contrôle de sécurité fondées sur les règles sont souvent vues comme une politique fondée sur des étiquettes de sécurité, avec des initiateurs possédant des autorisations telles que «secret» ou «technique», et des cibles protégées possédant des classifications nommées de la même façon.

Une politique de contrôle d'accès fondée sur l'identité est une politique dans laquelle les utilisateurs individuels ou les groupes ou les rôles se voient accorder ou dénier l'accès sur la base de leur identité ou leur information ACI.

Sur inspection, certaines des différences entre une politique de contrôle d'accès fondée sur les règles et une politique de contrôle d'accès fondée sur l'identité ne sont pas clairement séparées: les autorisations de la politique de contrôle d'accès fondée sur les règles et l'information ACI d'initiateur sont par essence les mêmes. Les autorisations liées à une politique de contrôle d'accès fondée sur les règles peuvent être considérées comme une information ACI d'initiateur particulière. En fait, si dans le cadre d'une politique fondée sur les règles des utilisateurs possèdent des autorisations individuelles uniques non hiérarchiques, les autorisations deviennent équivalentes aux identités d'utilisateur et les classifications de cible deviennent équivalentes à des entrées de liste de contrôle d'accès.

Une autre distinction souvent établie entre les politiques fondées sur les règles et fondées sur l'identité concerne le fait que les politiques fondées sur les règles sont administrativement appliquées alors que les politiques fondées sur l'identité sont sélectionnées par l'utilisateur. Dans les termes du cadre de sécurité, la distinction se situe dans le contrôle de l'accès à l'information ACI lorsque l'information ACI est elle-même considérée comme une cible (à des fins de modification). Cette distinction n'est pas clairement établie: il y a une variété de choix de distribution ou de centralisation possible pour le contrôle, en fonction de la politique de contrôle d'accès allant d'une simple politique imposée administrativement à une simple politique sélectionnée par l'utilisateur. Cela reflète les besoins du monde réel illustrés par les administrateurs de sécurité ou leurs agents (par exemple, responsables de département ou chefs d'équipe) versus les politiques de contrôle d'accès établies individuellement.

Annexe F

Un mécanisme pour mettre en œuvre l'envoi de l'information ACI par le biais d'un initiateur

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

Cette structure met en jeu trois entités:

- l'initiateur A;
- l'entité C;
- l'entité B.

Le but de cette structure est de permettre à un initiateur d'initier les transferts d'information directement de l'entité C vers l'entité B sans impliquer l'initiateur A durant la phase de transfert.

L'initiateur accède d'abord à l'entité C et fournit l'information ACI attachée à l'initiateur de sorte que l'accès puisse être accordé. Ensuite l'entité C fournit à l'initiateur l'information qui sera utilisée plus tard par l'entité B pour accéder à l'entité C. Elle est composée de deux parties:

- une référence unique à l'entité C durant la période de validité de la référence;
- une clé cryptographique protégée en utilisant un service de confidentialité entre l'entité C et l'initiateur.

Afin de réaliser un accès sur l'entité C, l'entité B a besoin d'obtenir de l'initiateur A la référence et la clé cryptographique. Lors de son transfert de l'initiateur vers l'entité B, la clé cryptographique est protégée en utilisant le service de confidentialité.

La référence et la clé cryptographique sont finalement utilisées pour générer l'information ACI attachée à la demande d'accès composée de la référence et de la valeur de contrôle cryptographique calculée en utilisant la clé cryptographique.

L'accès peut être alors accordé par l'entité C si la clé cryptographique utilisée pour produire la valeur de contrôle cryptographique correspond à celle qui est associée à la référence.

Annexe G

Grandes lignes du service de sécurité de contrôle d'accès

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

<table>
<tr><td colspan="3" rowspan="4">Grandes lignes du service de sécurité</td><td rowspan="3">Elément</td><td>Entités:</td><td colspan="3">initiateur, cible</td></tr>
<tr><td>Fonctions:</td><td colspan="3">fonction d'application de contrôle d'accès (AEF),
fonction de décision de contrôle d'accès (ADF)</td></tr>
<tr><td>Information:</td><td colspan="3">information de contrôle d'accès (ACI), information de décision de contrôle d'accès (ADI), information de contexte, règles de politique</td></tr>
<tr><td colspan="5">But des entités: interpréter l'information pour permettre aux initiateurs d'accéder seulement aux cibles autorisées</td></tr>
<tr><td rowspan="6">FONCTIONNALITÉS</td><td colspan="2" rowspan="2">Fonctionnalités liées à la gestion</td><td>Entité</td><td colspan="4">Autorité du domaine de sécurité (SDA)</td></tr>
<tr><td>Fonction</td><td colspan="4"></td></tr>
<tr><td colspan="5">– Installer l'information ACI
– Changer l'information ACI
– Révoquer l'information ACI
– Révoquer l'information ADI
– Lister l'information ACI
– Mettre hors service composant
– Remettre au service composant</td></tr>
<tr><td colspan="2" rowspan="3">Fonctionnalités opérationnelles apparentées</td><td>Entité</td><td colspan="2">Initiateur</td><td>Cible</td><td></td></tr>
<tr><td>Fonction</td><td colspan="2"></td><td></td><td>ADF</td></tr>
<tr><td colspan="2">– Identifier autorité distante
– Etablir politique d'interaction sécurisée
– Acquérir information ACI
– Générer information ACI
– Révoquer information ADI</td><td>– Acquérir information ACI
– Révoquer information ADI</td><td>– Acquérir information ACI
– Vérifier information ACI et dériver information ADI
– Obtenir information ACI de contexte
– Décider accès</td></tr>
<tr><td rowspan="3">INFORMATION</td><td colspan="2">Eléments de données gérés par l'autorité SDA</td><td colspan="5">– Identificateurs (autorité SDA, initiateur, cible, politique d'interaction sécurisée, groupes, rôles)
– Critères de sélection ACI
– Période de validité
– Marquage de sensibilité
– Marquage d'intégrité</td></tr>
<tr><td colspan="2">Information utilisée dans les opérations</td><td colspan="5">– Information ACI/ADI (initiateur, liée à l'initiateur, cible, liée à la cible, demande d'accès, liée à la demande d'accès, opérande, liée à l'opérande, échange, de contexte, retenue)
– Liste de contrôle d'accès
– Capacité
– Etiquette
– Certificat de contrôle d'accès
– Jeton de contrôle d'accès</td></tr>
<tr><td colspan="2">Information de contrôle</td><td colspan="5">– Intervalle de temps
– Etat du système
– Représentation de la politique de contrôle d'accès
– Teneur de l'authentification
– Route des communications</td></tr>
</table>