UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T X.841

(10/2000)

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

SÉRIE X: RÉSEAUX DE DONNÉES ET
COMMUNICATION ENTRE SYSTÈMES OUVERTS

Sécurité

Technologies de l'information – Techniques de sécurité – Objets d'information de sécurité pour le contrôle d'accès

Recommandation UIT-T X.841

(Antérieurement Recommandation du CCITT)

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES ET COMMUNICATION ENTRE SYSTÈMES OUVERTS

RÉSEAUX PUBLICS DE DONNÉES	
Services et fonctionnalités	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
Définitions 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 des couches	X.280–X.289
Tests de conformité	X.290–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	
Généralités	X.300–X.349
Systèmes de transmission de données par satellite	X.350–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	
Réseautage	X.600–X.629
Efficacité	X.630–X.639
Qualité de service	X.640–X.649
Dénomination, adressage et enregistrement	X.650–X.679
Notation de syntaxe abstraite numéro un (ASN.1)	X.680–X.699
GESTION OSI	
Cadre général et architecture de la gestion-systèmes	X.700–X.709
Service et protocole de communication de gestion	X.710–X.719
Structure de l'information de gestion	X.720–X.729
Fonctions de gestion et fonctions ODMA	X.730–X.799
SÉCURITÉ	**X.800–X.849**
APPLICATIONS OSI	
Engagement, concomitance et rétablissement	X.850–X.859
Traitement transactionnel	X.860–X.879
Opérations distantes	X.880–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

NORME INTERNATIONALE 15816

RECOMMANDATION UIT-T X.841

TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SECURITE – OBJETS D'INFORMATION DE SECURITE POUR LE CONTROLE D'ACCES

Résumé

La présente Recommandation | Norme internationale rassemble les définitions d'objets courantes utiles pour les normes de sécurité afin d'éviter la présence de définitions multiples et différentes de la même fonctionnalité. L'utilisation de la notation de syntaxe abstraite numéro un (ASN.1) a permis d'obtenir des définitions précises.

La présente Recommandation | Norme internationale ne couvre que les aspects statiques des objets d'information de sécurité (SIO).

Source

La Recommandation X.841 de l'UIT-T, élaborée par la Commission d'études 7 (1997-2000) de l'UIT-T, a été approuvée par l'Assemblée mondiale de normalisation des télécommunications (Montréal, 27 septembre – 6 octobre 2000). Un texte identique est publié comme Norme Internationale ISO/CEI 15816.

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. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies 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.

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.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un Membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux responsables de la mise en œuvre de consulter la base de données des brevets du TSB.

TABLE DES MATIÈRES

Introduction

La présente Recommandation | Norme internationale sur les objets d'information de sécurité pour le contrôle d'accès rassemble les définitions d'objets courantes utiles pour les normes de sécurité afin d'éviter la multiplicité de définitions différentes de la même fonctionnalité. Il a été possible d'obtenir des définitions précises grâce à l'utilisation de la notation de syntaxe abstraite numéro un (ASN.1) définie dans la Rec. UIT-T X.680 (1997) | ISO/CEI 8824-1:1998, et la Rec. UIT-T X.681 (1997) | ISO/CEI 8824-2:1998.

L'objet de la gestion de sécurité est de protéger de manière appropriée et économique le capital, y compris l'information. Afin de protéger leurs intérêts et leurs droits de propriété intellectuelle, les organisations doivent pouvoir contrôler la façon dont leur information est traitée. Le détenteur ou le créateur d'informations sensibles peut subir un préjudice considérable ou être dans une situation fort embarrassante si, par exemple, cette information est communiquée à des personnes non autorisées (rupture de confidentialité) ou si cette information est modifiée de manière quelconque (rupture d'intégrité). Chaque organisation doit s'efforcer de protéger son capital et notamment son information de manière adéquate et sous toutes ses formes pendant son stockage, son traitement et sa circulation interne et externe sur les réseaux privés ou publics. Les organisations doivent avoir l'assurance que leur capital sera bien protégé lorsque celui-ci sera détenu ou traité par des tiers si elles envisagent d'élargir leur activité.

L'élaboration des objets SIO pour le contrôle d'accès a été motivée par la recherche d'une souplesse et d'une interopérabilité dans la gestion de la sécurité découlant de l'utilisation de structures communes pour des fonctions similaires. Dans la présente Recommandation | Norme internationale, on s'est efforcé de normaliser des étiquettes de sécurité et diverses méthodes de contrôle d'accès.

NORME INTERNATIONALE

RECOMMANDATION UIT-T

TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – OBJETS D'INFORMATION DE SÉCURITÉ POUR LE CONTRÔLE D'ACCÈS

1 Domaine d'application

La présente Recommandation | Norme internationale s'applique à:

a) la définition de directives pour la spécification de la syntaxe abstraite des objets d'information de sécurité (SIO) génériques ou particuliers pour le contrôle d'accès;

b) la spécification des objets SIO génériques pour le contrôle d'accès;

c) la spécification d'objets SIO spécifiques pour le contrôle d'accès.

La présente Recommandation | Norme internationale ne couvre que les aspects "statiques" des objets SIO et utilise pour cela des définitions syntaxiques sous forme de descriptions ASN.1 et d'explications sémantiques additionnelles. Elle ne couvre pas les aspects "dynamiques" des objets SIO comme, par exemple, les règles relatives à leur création et à leur suppression. Les aspects "dynamiques" des objets SIO relèvent de la mise en œuvre locale.

2 Références normatives

Les Recommandations et 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.411 (1999) | ISO/CEI 10021-4:2001, *Technologies de l'information – Systèmes de messagerie: système de transfert de messages: définition et procédures du service abstrait.*

– Recommandation UIT-T X.500 (2001) | ISO/CEI 9594-1:2001, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: aperçu général des concepts, modèles et services.*

– Recommandation UIT-T X.501 (2001) | ISO/CEI 9594-2:2001, *Technologies de l'information – Interconnexion des systèmes ouverts – L'Annuaire: les modèles.*

– Recommandation UIT-T X.509 (2000) | ISO/CEI 9594-8:2001, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre général des certificats de clé publique et d'attribut.*

– Recommandation UIT-T X.680 (1997) | ISO/CEI 8824-1:1998, *Technologies de l'information – Notation de syntaxe abstraite numéro un: spécification de la notation de base.*

– Recommandation UIT-T X.681 (1997) | ISO/CEI 8824-2:1998, *Technologies de l'information – Notation de syntaxe abstraite numéro un: spécification des objets informationnels.*

– Recommandation UIT-T X.682 (1997) | ISO/CEI 8824-3:1998, *Technologies de l'information – Notation de syntaxe abstraite numéro un: spécification des contraintes.*

- Recommandation UIT-T X.683 (1997) | ISO/CEI 8824-4:1998, *Technologies de l'information – Notation de syntaxe abstraite numéro un: paramétrage des spécifications de la notation de syntaxe abstraite numéro un.*
- Recommandation UIT-T X.690 (1997) | ISO/CEI 8825-1:1998, *Technologies de l'information – Règles de codage ASN.1: spécification des règles de codage de base, des règles de codage canoniques et des règles de codage distinctives.*
- Recommandation CCITT X.722 (1992) | ISO/CEI 10165-4:1992, *Technologies de l'information – Interconnexion des systèmes ouverts – Structure de l'information de gestion: directives pour la définition des objets gérés.*
- Recommandation UIT-T X.741 (1995) | ISO/CEI 10164-9:1995, *Technologies de l'information – Interconnexion des systèmes ouverts – Gestion-Systèmes: objets et attributs pour le contrôle d'accès.*
- Recommandation UIT-T X.803 (1994) | ISO/CEI 10745:1995, *Technologies de l'information – Interconnexion des systèmes ouverts – Modèle de sécurité pour les couches supérieures.*
- 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.830 (1995) | ISO/CEI 11586-1:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Sécurité générique des couches supérieures: aperçu général, modèles et notation.*

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

- Recommandation CCITT X.800 (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT.*

  ISO 7498-2:1989, *Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Modèle de référence de base – Partie 2: architecture de sécurité.*

3 Définitions

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

3.1 **compartimentage**: définie dans l'ISO/CEI DIS 2382-8.

3.2 **classe générique de SIO**: classe de SIO dans laquelle les types de données pour l'une ou plusieurs des composantes ne sont pas totalement spécifiés.

3.3 **objet d'information**: défini dans la Rec. UIT-T X.681 | ISO/CEI 8824-2.

3.4 **classe d'objets d'information**: définie dans la Rec. UIT-T X.681 | ISO/CEI 8824-2.

3.5 **identificateur d'objet (OID)**: défini dans la Rec. UIT-T X.680 | ISO/CEI 8824-1.

3.6 **sceau**: défini dans la Rec. UIT-T X.810 | ISO/CEI 10181-1.

3.7 **autorité chargée de la sécurité**: entité responsable auprès de l'administration de la politique de sécurité dans un domaine de sécurité.

3.8 **domaine de sécurité**: ensemble d'utilisateurs et de systèmes faisant l'objet de l'application d'une politique de sécurité commune.

3.9 **objet d'information de sécurité**: instance d'une classe d'objets SIO.

3.10 **classe d'objets d'information de sécurité**: classe d'objets d'information qui a été adaptée pour une utilisation de sécurité.

3.11 **étiquette de sécurité**: défini dans la Recommandation CCITT X.800 et dans l'ISO 7498-2.

3.12 **politique de sécurité**: défini dans l'ISO/CEI DIS 2382-8.

3.13 **fichier d'informations sur la politique de sécurité**: structure qui achemine l'information sur la politique de sécurité propre au domaine.

3.14 **classe d'objets SIO spécifiques**: classe d'objets SIO dans laquelle les types de données pour toutes les composantes sont entièrement spécifiés.

4 Abréviations

Pour les besoins de la présente Recommandation | Norme internationale, les abréviations suivantes sont utilisées:

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

EE Entité d'extrémité

IT Technologies de l'information *(information technology)*

OID Identificateur d'objet *(object identifier)*

RBAC Contrôle d'accès réglementé (*rule based access control*)

SIO Objet d'information de sécurité *(security information object)*

SPIF Fichier d'informations sur la politique de sécurité *(security policy information file)*

5 Conventions

5.1 Description de la classe d'objets d'information de sécurité

Une classe d'objets SIO comprend:

- une valeur d'identificateur de classe SIO;
- un ensemble de spécifications de type de données, une par composante contenue dans la classe de SIO;
- une déclaration de la sémantique associée à l'utilisation de la classe de SIO.

5.2 Correspondance de classe générique d'objets d'information de sécurité

Une classe générique de SIO est une classe de SIO dans laquelle les types de données pour une ou plusieurs composantes ne sont pas totalement spécifiés. Une classe de SIO spécifique est une classe de SIO dans laquelle les types de données pour toutes les composantes sont intégralement spécifiés. Une classe générique de SIO correspond à une famille de classe de SIO spécifique.

5.3 Composition des objets d'information de sécurité

La spécification de chaque objet SIO dans la présente Recommandation | Norme internationale se compose des éléments suivants:

- une description du SIO;
- une explication de l'utilisation du SIO;
- une description des composantes du SIO.

La description des composantes du SIO inclut la spécification ASN.1 et l'identificateur d'objet de la classe d'objets en cours de définition.

6 Spécification des objets d'information de sécurité

Lorsque le besoin d'un nouvel objet SIO se fait sentir, il faut suivre les étapes suivantes si l'on veut faciliter la réutilisation des spécifications existantes et réduire la multiplication de différentes spécifications correspondant au même besoin:

- la définition contenue dans cette Recommandation | Norme internationale doit être utilisée lorsque la présente Recommandation | Norme internationale définit un objet SIO qui répond à un nouveau besoin;
- les composantes des objets SIO définis dans la présente Recommandation | Norme internationale doivent être utilisées pour la définition du nouvel objet SIO lorsqu'elles correspondent en partie au nouveau besoin.

Les spécifications des objets SIO qui ont été définis dans le but de prendre en charge le contrôle d'accès sont données dans les paragraphes qui suivent. Une définition complète en notation ASN.1 des objets d'information de sécurité qui sont traités dans ces paragraphes est donnée sous la forme d'un module à l'Annexe A. Ce module est identifié comme suit:

```
id-SIOsAccessControl-MODULE OBJECT IDENTIFIER ::= {
        joint-iso-itu-t sios(24) specification(0) modules(0) accessControl(0)}
```

6.1 Etiquettes de confidentialité

6.1.1 Introduction

Les organisations ont en général une ou plusieurs politiques de sécurité qui prévoient le compartimentage en groupe des données, données qui sont protégées et manipulées de la même façon. La politique de sécurité définit la protection à appliquer à chaque compartiment.

Les aspects sécurité exprimés par une politique de sécurité, indiqués dans une étiquette de sécurité se composent des éléments suivants:

- le niveau de protection à accorder aux données stockées dans un système;
- le nom des personnes qui sont autorisées à accéder aux données, processus ou ressources;
- les marquages de sécurité à afficher sur l'écran ou à imprimer sur la version papier avec les informations;
- les exigences en matière d'acheminement et de cryptage pour les données transmises entre systèmes;
- les exigences de protection contre les copies non autorisées;
- les méthodes de stockage des données;
- les algorithmes de cryptage à utiliser;
- les méthodes d'authentification des entités;
- une indication précisant si les opérations sur l'objet doivent être soumises à une vérification;
- une indication précisant si le destinataire d'un objet n'a pas la possibilité de le refuser;
- une indication précisant si des signatures numériques sont requises pour authentifier les données et quelles sont ces signatures.

Lorsque les données sont stockées sur un système utilisant les technologies de l'information (système IT), ou lorsqu'elles sont transmises électroniquement entre systèmes, les données sont étiquetées afin d'indiquer le compartiment de sécurité auquel elles appartiennent et aussi comment elles doivent être traitées en ce qui concerne la sécurité. L'étiquette peut être séparément identifiable de l'information protégée mais elle est logiquement liée à cette information. L'intégrité des étiquettes, et l'intégrité de leur lien avec l'information, doivent être garanties. Le système IT et le réseau peuvent ainsi prendre des décisions relatives à la sécurité, telles le contrôle d'accès et l'acheminement, sans qu'il soit nécessaire d'accéder à l'information protégée. L'étiquette de sécurité peut être associée à chaque objet données dans un système IT (documents, courrier électronique, fenêtres d'affichage, entrées aux bases de données, entrées aux annuaires et formulaires électroniques, etc.). Les étiquettes sont destinées à être utilisées lorsque les objets sont stockés, déplacés (particulièrement entre systèmes), et lorsqu'ils doivent être manipulés par des applications qui agissent sur des étiquettes, y compris les applications qui créent de nouveaux objets à partir des objets existants.

Lorsque les données étiquetées doivent être transmises entre différents domaines de sécurité, les domaines doivent décider de la politique de sécurité à appliquer à ces données. Si les étiquettes spécifiées par la politique appliquée à l'intérieur d'un domaine diffèrent des étiquettes spécifiées par la politique pour les données utilisées en commun, la politique applicable aux données utilisées en commun doit spécifier comment effectuer la conversion entre les deux ensembles d'étiquettes.

Les étiquettes elles-mêmes ne suffisent pas à assurer la sécurité de l'information. La politique de sécurité en matière d'information doit être mise en vigueur par chaque organisation lorsque l'information étiquetée relève de leur compétence. Toutes les organisations, personnes et systèmes IT qui manipulent un élément d'information sont supposés connaître la politique de sécurité applicable à cette information. Des organisations qui échangent de l'information doivent avoir une confiance mutuelle, garantissant que cette information sera manipulée conformément aux politiques de sécurité convenues. Cette confiance fait en général l'objet d'un accord formel.

6.1.2 Spécification ASN.1 de l'étiquette

L'étiquette de confidentialité est identifiée comme suit:

```
id-ConfidentialityLabel OBJECT IDENTIFIER  ::= {
        joint-iso-itu-t sios(24) specification(0) securityLabels(1) confidentiality(0)}

ConfidentialityLabel  ::=  SET {
          security-policy-identifier        SecurityPolicyIdentifier OPTIONAL,
          security-classification           INTEGER(0..MAX) OPTIONAL,
          privacy-mark                      PrivacyMark OPTIONAL,
          security-categories               SecurityCategories OPTIONAL }
(ALL EXCEPT({-- néant; une composante au moins doit être présente --}))
```

```
SecurityPolicyIdentifier ::= OBJECT IDENTIFIER

PrivacyMark ::= CHOICE {
  pString                PrintableString (SIZE(1..ub-privacy-mark-length)),
  utf8String             UTF8String (SIZE(1..ub-privacy-mark-length))
}

ub-privacy-mark-length INTEGER ::= 128 -- comme défini dans la Rec. UIT-T X.411 | ISO/CEI 10021-4

SecurityCategories ::= SET SIZE (1..MAX) OF SecurityCategory

SecurityCategory ::= SEQUENCE {
     type [0]   SECURITY-CATEGORY.&id ({SecurityCategoriesTable}),
     value      [1]   SECURITY-CATEGORY.&Type ({SecurityCategoriesTable} {@type})
}

SECURITY-CATEGORY ::= TYPE-IDENTIFIER

SecurityCategoriesTable SECURITY-CATEGORY ::= {…}
```

Un exemple de développement de la classe d'objets d'information TYPE-IDENTIFIER est donné dans l'Annexe B.

6.1.3 Méthode d'établissement de lien pour les étiquettes de confidentialité

6.1.3.1 Méthode 1

Une copie des données (D) et une copie de l'étiquette de sécurité (L) sont stockées ensemble, dans un enregistrement de données, dans des limites sécurisées du système. On suppose que le système assure la protection de l'intégrité de l'étiquette de sécurité, l'intégrité des données, ainsi qu'éventuellement leur secret. La protection offerte par le système doit être telle qu'un utilisateur non autorisé ou une application non autorisée ne puisse pas modifier les données ou leur étiquette de sécurité. Avec cette méthode d'établissement d'un lien, il n'est pas nécessaire d'avoir une fonction cryptographique pour lier les données et l'étiquette de sécurité.

6.1.3.2 Méthode 2

Une signature numérique non secrète (S) est calculée sur D (données) et L (étiquette) au moyen d'un algorithme de signature numérique (SigAlg) et la clé privée (X) d'un algorithme à clé publique, à savoir:

$$S = SigAlg(X,f(D),L)$$

La signature numérique est stockée avec D et L dans un même enregistrement de données. La signature numérique ainsi générée lie L à D. Dans cette définition, f est une fonction publique telle que f(D) ne révèle pas l'information concernant D.

Dans cette méthode d'établissement d'un lien, L et S ne doivent pas être nécessairement stockés dans les limites sécurisées du système. Lorsqu'un service cryptographique est sollicité avec une valeur incorrecte de L, D ou S, l'incohérence est détectée. Cette détection est effectuée au moyen d'une clé publique de l'algorithme de clé publique servant de clé de vérification de la signature.

6.1.3.3 Méthode 3

Un code d'authentification de message (MAC) non secret est calculé sur D et L au moyen d'un mode de génération de code MAC d'un algorithme de cryptage (MacAlg) et une clé d'algorithme MAC secrète (K-MAC), à savoir:

$$MAC = MacAlg(K\text{-}MAC,f(D),L)$$

Le code MAC est stocké avec D et L dans un enregistrement de données. Le code MAC ainsi généré lie L à D. Dans cette définition, f est une fonction publique de sorte que f(D) ne révèle pas l'information concernant D.

Dans cette méthode d'établissement de lien, L et MAC ne doivent pas nécessairement être stockés dans la limite sécurisée d'un système. Lorsqu'un service cryptographique est sollicité avec une valeur non correcte de L, D ou MAC, l'incohérence est détectée. Cette détection est faite en calculant un code MAC de référence utilisant les valeurs fournies de L et de D et une copie de K-MAC, puis en comparant les résultats avec le code MAC fourni.

6.2 Fichier d'information sur la politique de sécurité

6.2.1 Introduction

Une politique de sécurité est la forme la plus simple d'un ensemble de critères de fourniture de services de sécurité. En ce qui concerne le contrôle d'accès, une politique de sécurité est un sous-ensemble d'une politique de sécurité à un niveau plus élevé du système qui définit le moyen d'appliquer les politiques de contrôle d'accès entre des initiateurs et des cibles. Le mécanisme de contrôle d'accès doit:

- permettre la communication lorsqu'une politique spécifique le permet;
- empêcher toute communication lorsqu'une politique spécifique ne le permet pas explicitement.

Une politique de sécurité forme la base des décisions prises par des mécanismes de contrôle d'accès. Une information de politique de sécurité propre au domaine considéré est acheminée via le fichier d'informations sur la politique de sécurité (SPIF, *security policy information file*).

Le fichier SPIF contient une séquence des éléments suivants:

- **versionInformation**: indique la version de la syntaxe ASN.1 et la sémantique associée de spécification du fichier SPIF.
- **updateInformation**: précise la validité des données du fichier SPIF.
- **securityPolicyIdData**: identifie la politique de sécurité à laquelle le fichier SPIF s'applique.
- **privilegeId**: indique l'identificateur d'objet OID qui identifie la syntaxe incluse dans la catégorie de sécurité de l'attribut d'autorisation des certificats sur lequel reposent les certificats utilisés en association avec le fichier SPIF. La syntaxe indiquée par **privilegeId** doit être homogène avec celle de **rbacId**.
- **securityClassifications**: mappe la classification de l'étiquette de sécurité avec la classification dans l'attribut d'autorisation, et indique les équivalences.
- **rbacId**: identificateur de contrôle d'accès basé sur des règles qui identifient la syntaxe incluse dans la catégorie de sécurité securityLabel qui est utilisée en association avec le fichier SPIF. La syntaxe indiquée par **rbacId** doit être homogène avec celle indiquée par **privilegeId**.
- **securityCategories**: mappe les catégories de sécurité d'une étiquette de sécurité sur des catégories de sécurité dans l'attribut d'autorisation et indique les équivalences.
- **equivalentPolicies**: regroupe toutes les politiques équivalentes dans le SPIF.
- **defaultSecurityPolicyIdData**: identifie la politique de sécurité lorsque les données sont reçues sans une étiquette de sécurité.
- **extensions**: définit un mécanisme permettant d'inclure les capacités additionnelles au fur et à mesure que de nouveaux besoins seront identifiés.

Le fichier SPIF est un objet signé protégé contre des modifications non autorisées.

6.2.2 Spécification ASN.1 du fichier d'information sur la politique de sécurité

Le fichier d'informations sur la politique de sécurité est défini par la syntaxe suivante:

```
SecurityPolicyInformationFile ::= SIGNED {EncodedSPIF}

EncodedSPIF ::= TYPE-IDENTIFIER.&Type( SPIF )

SPIF ::= SEQUENCE    {
        versionInformation                  VersionInformationData DEFAULT v1,
        updateInformation                   UpdateInformationData,
        securityPolicyIdData                ObjectIdData,
        privilegeId                         OBJECT IDENTIFIER,
        rbacId                              OBJECT IDENTIFIER,
        securityClassifications     [0]     SEQUENCE OF SecurityClassification OPTIONAL,
        securityCategories          [1]     SEQUENCE OF SecurityCategory OPTIONAL,
```

```
equivalentPolicies              [2]     SEQUENCE OF EquivalentPolicy OPTIONAL,
defaultSecurityPolicyIdData     [3]     ObjectIdData OPTIONAL,
extensions                      [4]     Extensions OPTIONAL }
```

6.2.2.1 Information sur la version

Le champ **versionInformation** indique la version de la syntaxe ASN.1 ainsi que la sémantique associée utilisées.

```
VersionInformationData ::= INTEGER { v1(0) } (0..MAX)
```

6.2.2.2 Information de mise à jour

Le champ **updateInformationData** est une séquence d'information propre à une version des données SPIF. Le **sPIFVersionNumber** différencie les diverses versions du fichier SPIF pour la politique de sécurité identifiée dans **securityPolicyIdData** dans le fichier SPIF. **CreationDate** indique lorsque le fichier SPIF a été généré. **OriginatorDistinguishedName** identifie le signataire du fichier SPIF. L'identificateur **keyIdentifier** identifie la clé utilisée pour signer le fichier SPIF.

```
UpdateInformationData ::= SEQUENCE    {
        sPIFVersionNumber               INTEGER (0..MAX),
        creationDate                    GeneralizedTime,
        originatorDistinguishedName     Name,
        keyIdentifier                   OCTET STRING OPTIONAL }
```

6.2.2.3 Données d'identification de la politique de sécurité

Le champ **securityPolicyIdData** identifie la politique de sécurité à laquelle le fichier SPIF s'applique. **SecurityPolicyIdData** est défini comme un **ObjectIdData**, lequel **ObjectIdData** est une séquence d'**objectId** et d'**objectIdName**. Un **objectId** est l'identificateur d'objet (OID) assigné à un objet spécifique, tandis que **objectIdName** est une chaîne identifiant un objet spécifique.

```
ObjectIdData ::= SEQUENCE {
        objectId                OBJECT IDENTIFIER,
        objectIdName            ObjectIdName }
ObjectIdName ::= DirectoryString {ubObjectIdNameLength}
```

6.2.2.4 Identificateur de privilèges

L'identificateur d'objet **privilegeId** identifie la syntaxe incluse dans la catégorie de sécurité de l'attribut d'autorisation des certificats justificatifs utilisés en association avec le fichier SPIF.

6.2.2.5 Identificateur de RBAC

L'identificateur d'objet **rbacId** identifie la syntaxe qui est incluse dans les catégories de sécurité **securityLabel** utilisées en association avec le fichier SPIF. La syntaxe utilisée par **rbacId** doit être homogène avec celle indiquée par **privilegeId**.

6.2.2.6 Classification de sécurité

Une SEQUENCE **SecurityClassification** est présente dans le fichier SPIF pour chaque valeur de classification de sécurité définie pour la politique de sécurité identifiée dans **securityPolicyIdData**. Il s'agit d'un élément facultatif (OPTIONAL).

Le champ **labelAndCertValue** représente la valeur assignée à cette classification dans l'étiquette de sécurité et la valeur entière représentant la position binaire de cette classification de sécurité dans la chaîne **classList BIT STRING** de l'attribut d'autorisation.

classificationName est une chaîne identifiant cette classification utilisée par l'application afin de déterminer le texte à afficher à l'utilisateur lorsqu'il choisit ou affiche la valeur de classification dans une étiquette de sécurité.

equivalentClassifications est une séquence de valeurs de classification (définies dans les politiques de sécurité autres que **securityPolicyIdData**) qui est équivalente au **SecurityClassification labelAndCertValue**.

hierarchyValue indique la position relative du **SecurityClassification labelAndCertValue d**ans la hiérarchie des classifications de sécurité dans la politique de sécurité indiquée par **securitypolicyIdData**. **hierarchyValue** doit être unique au sein de la politique de sécurité.

markingData identifie l'information de marquage attaché à l'objet donné. **markingData** est composé de chaînes et de codes de marquage qui identifient les endroits où la chaîne est physiquement affichée. Si la **markingPhrase** est absente, le **markingCode** s'applique au **SecurityClassification classificationName**.

Lorsqu'une catégorie de sécurité ou une classification de sécurité est choisie pour inclusion dans l'étiquette de sécurité, le champ associé du **requiredCategory** du fichier SPIF, s'il est présent, indique les catégories de sécurité qui doivent être également incluses dans l'étiquette de sécurité en association avec la valeur sélectionnée. Si le champ **requiredCategory** n'est pas présent, la valeur sélectionnée n'a pas de dépendance avec une catégorie de sécurité quelconque.

Si l'opération **OptionalCategoryGroup** est **onlyOne**, alors une (et une seule) catégorie de sécurité incluse dans **categoryGroup** doit être incluse dans l'étiquette de sécurité. Si l'opération **OptionalCategoryGroup** est **oneOrMore**, alors une ou plusieurs catégories de sécurité incluses dans **categoryGroup** doivent être incluses dans l'étiquette de sécurité. Si l'opération **OptionalCategoryGroup** est all, alors toutes les catégories de sécurité incluses dans **categoryGroup** doivent être incluses dans l'étiquette de sécurité. L'utilisateur doit choisir chaque valeur. Si plusieurs **OptionalCategoryGroups** sont présents dans **requiredCategories**, alors la condition à satisfaire exprimée par tous les **OptionalCategoryGroups** doit être satisfaite. **categoryGroup** est une séquence de **OptionalCategoryData**. L'identificateur d'objet **optCatDataId** doit spécifier une syntaxe à utiliser dans le champ **OptionalCategoryData categorydata** qui est homogène avec ceux spécifiés par les identificateurs d'objet de type **rbacId, privilegeId** et SecurityCategory du fichier SPIF.

La composante **obsolete**, lorsque qu'elle est mise à TRUE, indique qu'une classification précédemment valide est devenue obsolète. Une telle classification peut être associée avec des objets de données anciens, mais ne doit pas être associée avec les nouveaux objets.

```
SecurityClassification ::= SEQUENCE {
        labelAndCertValue                   LabelAndCertValue,
        classificationName                  ClassificationName,
        equivalentClassifications   [0]     EquivalentClassifications OPTIONAL,
        hierarchyValue                      INTEGER,
        markingData                 [1]     MarkingDataInfo OPTIONAL,
        requiredCategory            [2]     OptionalCategoryGroups OPTIONAL,
        obsolete                            BOOLEAN DEFAULT FALSE       }

LabelAndCertValue ::= INTEGER (0..MAX)
ClassificationName ::= DirectoryString { ubClassificationNameLength }
EquivalentClassifications ::= SEQUENCE SIZE(0..MAX) OF EquivalentClassification

EquivalentClassification ::= SEQUENCE {
        securityPolicyId            OBJECT IDENTIFIER,
        labelAndCertValue           LabelAndCertValue,
        applied Applied }

Applied ::= INTEGER {
        encrypt (0),
        decrypt (1),
        both    (2) }
 (encrypt | decrypt | both)

MarkingDataInfo ::= SEQUENCE SIZE(1..MAX) OF MarkingData

MarkingData ::= SEQUENCE {
        markingPhrase               MarkingPhrase OPTIONAL,
        markingCodes                MarkingCodes OPTIONAL }
  (ALL EXCEPT({-- néant; une composante au moins doit être présente --}))

MarkingPhrase ::= DirectoryString { ubMarkingPhraseLength }

MarkingCodes ::= SEQUENCE SIZE(1..MAX) OF MarkingCode

MarkingCode ::= INTEGER {
        pageTop                     (1),
        pageBottom                  (2),
        pageTopBottom               (3),
        documentEnd                 (4),
        noNameDisplay               (5),
        noMarkingDisplay            (6),
        unused                      (7),
        documentStart               (8),
        suppressClassName           (9) }

OptionalCategoryGroups ::= SEQUENCE SIZE(1..MAX) OF OptionalCategoryGroup

OptionalCategoryGroup ::= SEQUENCE {
        operation                   Operation,
        categoryGroup               CategoryGroup }
```

```
Operation ::= INTEGER {
        onlyOne                 (1),
        oneOrMore               (2),
        all                     (3)}
(onlyOne | oneOrMore | all)

CategoryGroup ::= SEQUENCE SIZE(1..MAX) OF OptionalCategoryData
OptionalCategoryData ::= SEQUENCE {
        optCatDataId            OC-DATA.&id({CatData}),
        categorydata            OC-DATA.&Type({CatData}{@optCatDataId }) }

OC-DATA ::= TYPE-IDENTIFIER
CatData OC-DATA ::= { ... }
```

6.2.2.7 Catégories de sécurité

Une séquence **SecurityCategory** est présente dans le fichier SPIF pour chaque catégorie de sécurité définie pour la politique de sécurité identifiée dans **securityPolicyIdData**. La syntaxe **SecurityCategory** est définie dans l'étiquette de confidentialité donnée au § 6.1. La syntaxe définie à utiliser dans le champ de valeur **SecurityCategory** qui est indiqué dans l'identificateur objet de type **SecurityCategory** doit être homogène avec les syntaxes indiquées par les identificateurs d'objets **privilegeId, rbacId** et **optCatDataID**.

6.2.2.8 Politiques équivalentes

equivalentPolicies est une liste de toutes les politiques de sécurité pour lesquelles des valeurs ont été incluses dans le fichier SPIF comme valeurs équivalentes. L'identificateur **securityPolicyId** est un identificateur d'objet qui identifie la politique de sécurité équivalente. Le nom **securityPolicyName** est une chaîne d'annuaires facultative identifiant le nom de la politique de sécurité équivalente.

```
EquivalentPolicy ::= SEQUENCE {
        securityPolicyId        OBJECT IDENTIFIER,
        securityPolicyName      SecurityPolicyName  OPTIONAL}

SecurityPolicyName ::= DirectoryString {ubObjectIdNameLength}
```

6.2.2.9 Identificateur de politique de sécurité par défaut

La valeur de **defaultSecurityPolicyIdData** prend en charge l'interopérabilité avec des applications qui ne prennent pas en charge le contrôle d'accès. Il est fait appel à cet identificateur d'objet lorsque aucune étiquette de sécurité n'est utilisée.

Il convient de noter que la politique de sécurité par défaut sera mappé sur un niveau de classification unique. Lorsqu'une valeur de classification de sécurité est mappée sur la politique de sécurité par défaut, la séquence **SecurityClassification** dans le fichier SPIF pour la valeur désignée inclura la séquence **equivalentClassification** dans laquelle l'identificateur **policyId** a la valeur de l'identificateur d'objet politique de sécurité par défaut.

6.2.2.10 Extensions

Le champ **extension** est une séquence d'information qui permet une expansion future du fichier SPIF à mesure que des besoins additionnels sont identifiés tout en maintenant l'interopérabilité avec les précédentes implémentations du fichier SPIF. Il contient les composantes **extnId, critical,** et **extnValue**. La syntaxe est importée de la Rec. UIT-T X.509 | ISO/CEI 9594-8.

Une extension peut être indiquée comme critique ou non critique. Un système utilisant le fichier SPIF DOIT rejeter le fichier SPIF s'il se trouve en présence d'une extension critique qu'il ne reconnaît pas; toutefois, une extension non critique peut être ignorée si elle n'est pas reconnue. Il convient de prendre certaines précautions lorsqu'on adopte des extensions critiques qui peuvent empêcher l'utilisation dans un contexte général.

```
Extensions ::= SEQUENCE OF Extension

Extension ::= SEQUENCE {
        extnId                  EXTENSION.&id ({ExtensionSet}),
        critical                BOOLEAN DEFAULT FALSE,
        extnValue               OCTET STRING
          -- contient un codage DER d'une valeur du type &ExtnType
          -- pour l'objet d'extension identifié par  extnId -- }

ExtensionSet EXTENSION ::= { ... }
```

```
EXTENSION  ::=  CLASS {
        &id                                OBJECT IDENTIFIER UNIQUE,
        &ExtnType }
WITH SYNTAX { SYNTAX &ExtnType IDENTIFIED BY &id }
```

6.3 Attribut clearance (autorisation)

6.3.1 Introduction

L'attribut clearance est utilisé pour définir des autorisations accordées à un utilisateur spécifique ou à une entité d'application. Les autorisations accordées à un utilisateur ou à une entité d'application peuvent être un sous-ensemble de la politique de sécurité totale de l'organisation (ou de ses politiques). De même, les autorisations peuvent englober la politique de sécurité dans sa totalité.

L'attribut clearance contient trois composantes: **policyId**, **classList**, et, facultativement, **securityCategory** comme le montre la Figure 1 ci-dessous.

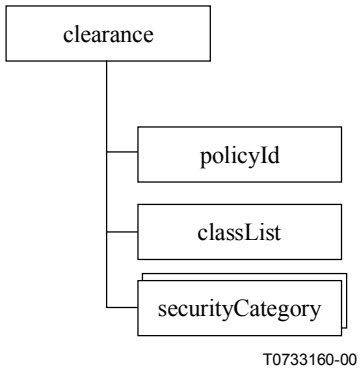

Figure 1 – Structure de l'attribut clearance

L'identificateur OID **policyId** identifie les composantes facultatives qui doivent être présentes. La composante **classList** définit les autorisations accordées à l'utilisateur et les autorisations hiérarchiques indiquées par **ClassList**, qui est définie dans la Rec. UIT-T X.501 | ISO/CEI 9594-2. Les autres listes de classes non hiérarchiques pourraient être définies ailleurs pour inclusion dans d'autres objets SIO ou traitées dans les catégories de sécurité. La composante **securityCategory** identifie tout numéro de catégorie de sécurité restrictive ou permissive mappée en bit ainsi que les catégories de sécurité restrictives et permissives énumérées assignées à l'utilisateur. Cette structure est illustrée à la Figure 2.

clearance

Sequence

policyId	**classList**		**securityCategory (optional)**
OID identificateur d'objet identifiant la politique de sécurité	unmarked unclassified restricted confidential secret topSecret	(0) (1) (2) (3) (4) (5)	Autorisations définies pour un domaine: – Accès permis (l'EE doit en avoir une) – Accès restreint (l'EE doit en avoir la totalité) – Accès numéroté (ex: accès national)

T0733170-00

Figure 2 – Champs de l'attribut clearance

6.3.2 Définition de l'attribut clearance

L'attribut clearance est défini comme suit:

```
clearance  ATTRIBUTE  ::=  { WITH SYNTAX    Clearance
        ID                                  id-at-clearance }

id-at-clearance OBJECT IDENTIFIER  ::=  {
  joint-iso-itu-t (2) ds (5) attributeType (4) clearance (55) }

Clearance  ::=  SEQUENCE {
        policyId                    OBJECT IDENTIFIER,
        classList                   ClassList DEFAULT {unclassified},
        securityCategories          SecurityCategories  OPTIONAL}

ClassList  ::=  BIT STRING {
        unmarked                    (0),
        unclassified                (1),
        restricted                  (2),
        confidential                (3),
        secret                      (4),
        topSecret                   (5)    }

SecurityCategories  ::=  SET SIZE(1..MAX) OF SecurityCategory
   -- SecurityCategory est définie dans l'étiquette de confidentialité qui est donnée au § 6.1.2
```

7 Interaction des objets d'information de sécurité

7.1 Comparaison de la structure de classe des objets SIO

La Figure 3 représente les structures de l'étiquette de confidentialité, de l'attribut clearance Rec. UIT-T X.501 | ISO/CEI 9594-2 et le fichier SPIF aux fins de comparaison. Les composantes équivalentes dans ces structures peuvent être examinées dans un logiciel d'application afin d'obtenir une fonctionnalité spécifique. L'obtention de ces fonctionnalités de contrôle d'accès utilisant ces structures est examinée au § 7.2.

7.2 Interaction des objets d'information de sécurité pour le contrôle d'accès

Le contrôle d'accès inclut le concept d'acheminement des autorisations pour les déclencheurs ou les utilisateurs ou bien l'utilisation d'un attribut d'autorisation et l'assignation des sensibilités à des objets cibles au moyen d'une étiquette de sécurité. Le fichier SPIF est utilisé pour interpréter ces autorisations et les paramètres de sensibilité. Le logiciel d'application utilise le fichier SPIF pour associer les sensibilités aux cibles, lire les sensibilités sur les étiquettes, lire et émettre des autorisations dans les certificats, et valider les mappages des politiques dans les domaines de politiques de sécurité.

Pour acheminer les autorisations et les sensibilités, on utilise des mécanismes de classification et de catégorie. Les classifications et les catégories sont formulées dans un attribut d'autorisation intégré dans le certificat d'utilisateur acheminant les autorisations à l'utilisateur considéré. Les classifications et les catégories sont également déclarées dans une étiquette de sécurité de l'objet qui de ce fait acheminent les sensibilités de cet objet. L'accès à un objet est permis lorsque les autorisations acheminées dans un attribut d'autorisation d'un utilisateur sont suffisantes au regard des sensibilités acheminées dans l'étiquette de sécurité de l'objet cible. La Figure 4 illustre les interactions parmi les objets SIO définis ici afin de permettre le contrôle d'accès dans un environnement de stockage de documents. Les autorisations figurant dans l'attribut d'autorisation du propriétaire des données, contenues dans le certificat concernant ce propriétaire des données, délimitent les autorisations extraites du fichier SPIF que le propriétaire peut déclarer dans l'étiquette pour les données cibles. L'étiquette est liée aux données et est stockée. Lors de l'accès aux données dans le dispositif de stockage, l'attribut d'autorisation de l'utilisateur, contenu dans le certificat concernant cet utilisateur, est comparé avec l'étiquette associée aux données cibles dans la fonction décision de contrôle d'accès. Si des sensibilités permissives sont présentes dans l'étiquette de sécurité, elles sont vérifiées afin de garantir qu'au moins une de ces sensibilités, présentes dans chaque partie permissive dans l'étiquette de sécurité, est également autorisée dans le certificat (autorisation(s) permissive(s)) permettant l'accès à l'objet données cibles par la fonction application de la commande d'accès. Un scénario de commande d'accès analogue pour un environnement de messagerie est représenté à la Figure 5.

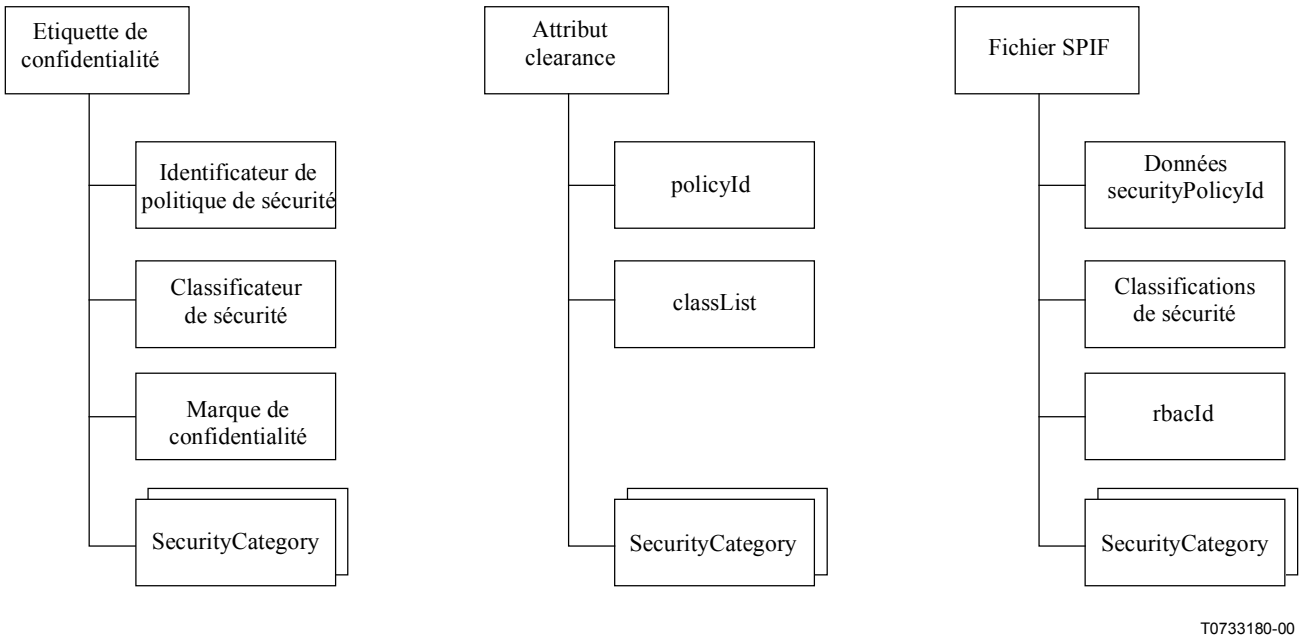

Figure 3 – Comparaison des classes d'objets équivalents

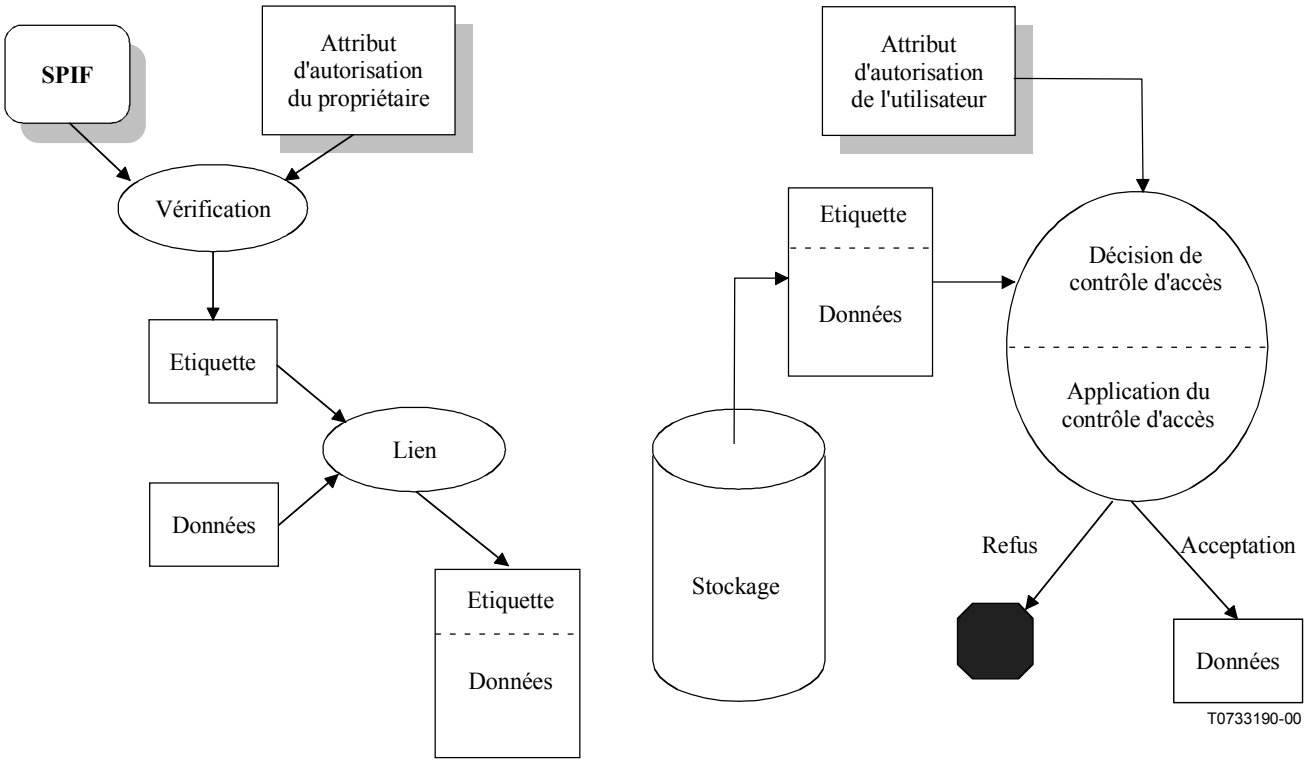

Figure 4 – Contrôle d'accès au stockage de données

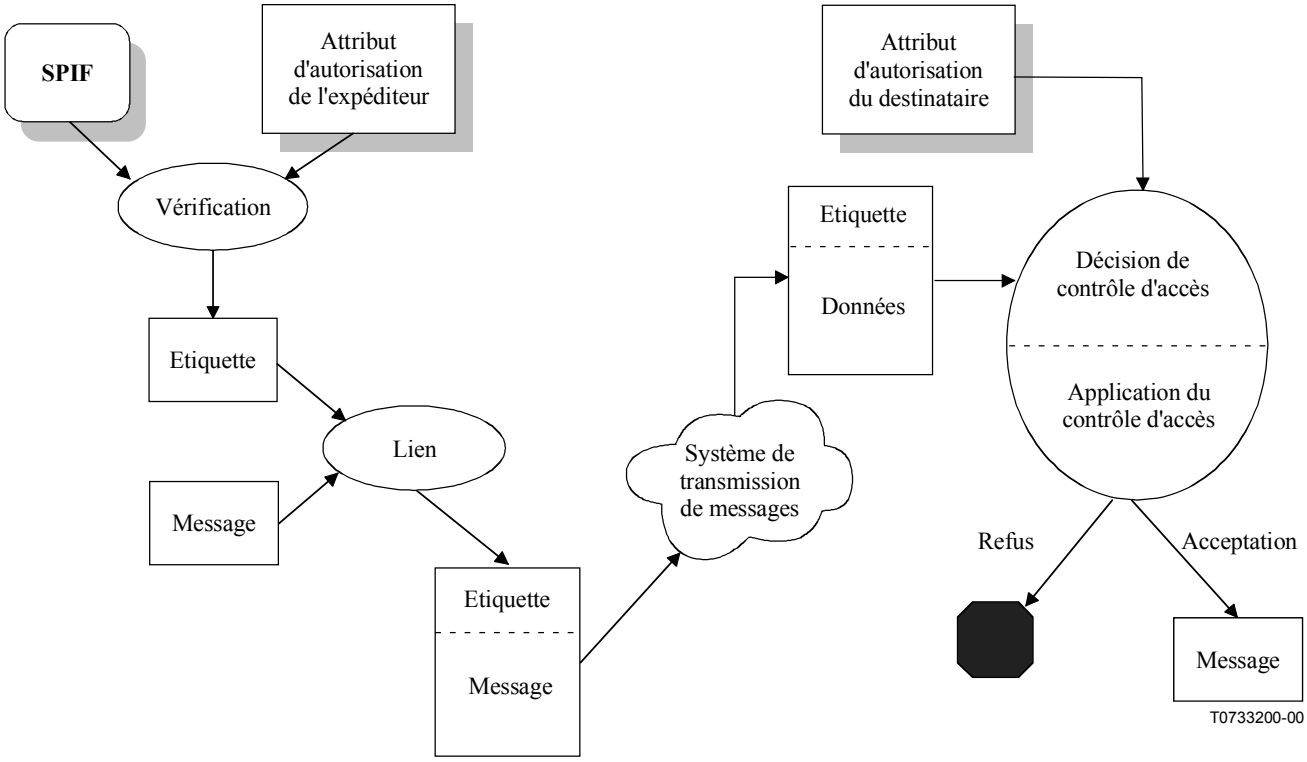

Figure 5 – Contrôle d'accès dans un scénario de messagerie

Annexe A

Objets d'information de sécurité pour le contrôle d'accès en ASN.1

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

La présente annexe contient sous la forme d'un module en ASN.1 toutes les définitions du type, de la valeur et de la classe d'objets d'information figurant dans la présente Recommandation | Norme internationale.

```
SIOsAccessControl-MODULE  {
   joint-iso-itu-t sios(24) specification(0) modules(0) accessControl(0)
}
       DEFINITIONS IMPLICIT TAGS ::= BEGIN

-- EXPORTS All; --

IMPORTS

   id-at-clearance
      FROM EnhancedSecurity        -- Rec. UIT-T X.501 | ISO/CEI 9594-2 --

   ATTRIBUTE, Name
      FROM InformationFramework    -- Rec. UIT-T X.501 | ISO/CEI 9594-2 --

   Extensions
      FROM CertificateExtensions   -- Rec. UIT-T X.509 | ISO/CEI 9594-8 --

   DirectoryString {}
      FROM SelectedAttributeTypes; -- Rec. UIT-T X.520 | ISO/CEI 9594-6 --

id-ConfidentialityLabel OBJECT IDENTIFIER  ::=  {joint-iso-itu-t sios(24) specification(0)
securityLabels(1) confidentiality(0)}

ConfidentialityLabel  ::=  SET {
   security-policy-identifier  SecurityPolicyIdentifier  OPTIONAL,
   security-classification     INTEGER(0..MAX)  OPTIONAL,
   privacy-mark                PrivacyMark  OPTIONAL,
   security-categories         SecurityCategories  OPTIONAL
}
 (ALL EXCEPT({-- néant; une composante au moins doit être présente --}))

SecurityPolicyIdentifier ::= OBJECT IDENTIFIER
```

```
PrivacyMark ::= CHOICE {
   pString     PrintableString (SIZE(1..ub-privacy-mark-length)),
   utf8String  UTF8String (SIZE(1..ub-privacy-mark-length))
}

ub-privacy-mark-length INTEGER ::= 128  -- comme défini dans X.411

SecurityCategories ::= SET SIZE(1..MAX) OF SecurityCategory

SecurityCategory ::= SEQUENCE {
   type   [0] SECURITY-CATEGORY.&id({SecurityCategoriesTable}),
   value  [1] EXPLICIT SECURITY-CATEGORY.&Type(
                              {SecurityCategoriesTable}{@type})
}

SECURITY-CATEGORY ::= TYPE-IDENTIFIER

SecurityCategoriesTable SECURITY-CATEGORY ::= {
   ...  -- objets définis selon les besoins --
}

SecurityPolicyInformationFile ::= SIGNED { EncodedSPIF }

-- Le type EncodedSPIF est un type ouvert dont la valeur est nécessairement
-- du type SPIF. Cette représentation de type ouvert est une chaîne opaque
-- de caractères hexadécimaux convenant aux opérations de signature
-- et de vérification de signature.

EncodedSPIF ::= TYPE-IDENTIFIER.&Type( SPIF )

SPIF ::= SEQUENCE {
   versionInformation           VersionInformationData  DEFAULT v1,
   updateInformation            UpdateInformationData,
   securityPolicyIdData         ObjectIdData,
   privilegeId                  OBJECT IDENTIFIER,
   rbacId                       OBJECT IDENTIFIER,
   securityClassifications      [0] SecurityClassifications  OPTIONAL,
   securityCategories           [1] SPIF-SecurityCategories  OPTIONAL,
   equivalentPolicies           [2] EquivalentPolicies  OPTIONAL,
   defaultSecurityPolicyIdData  [3] ObjectIdData  OPTIONAL,
   extensions                   [4] Extensions  OPTIONAL
}
```

```
VersionInformationData ::= INTEGER { v1(0) } (0..MAX)

UpdateInformationData ::= SEQUENCE {
   sPIFVersionNumber            SPIFVersionNumber,
   creationDate                 GeneralizedTime,
   originatorDistinguishedName  Name,
   keyIdentifier                OCTET STRING  OPTIONAL
}

SPIFVersionNumber ::=  INTEGER (0..MAX)

ObjectIdData ::= SEQUENCE {
   objectId      OBJECT IDENTIFIER,
   objectIdName  ObjectIdName
}

ObjectIdName ::= DirectoryString { ubObjectIdNameLength }

SecurityClassifications ::=
      SEQUENCE SIZE(0..MAX) OF SecurityClassification

SPIF-SecurityCategories ::=
      SEQUENCE SIZE(0..MAX) OF SecurityCategory

EquivalentPolicies ::=
      SEQUENCE SIZE(0..MAX) OF EquivalentPolicy

SecurityClassification ::= SEQUENCE {
   labelAndCertValue          LabelAndCertValue,
   classificationName         ClassificationName,
   equivalentClassifications  [0] EquivalentClassifications  OPTIONAL,
   hierarchyValue             INTEGER,
   markingData                [1] MarkingDataInfo  OPTIONAL,
   requiredCategory           [2] OptionalCategoryGroups  OPTIONAL,
   obsolete                   BOOLEAN  DEFAULT FALSE
}

LabelAndCertValue ::= INTEGER(0..MAX)

ClassificationName ::= DirectoryString { ubClassificationNameLength }
EquivalentClassifications ::=
     SEQUENCE SIZE(0..MAX) OF EquivalentClassification
```

```
EquivalentClassification ::= SEQUENCE {
   securityPolicyId   OBJECT IDENTIFIER,
   labelAndCertValue  LabelAndCertValue,
   applied            Applied
}

Applied ::= INTEGER {
   encrypt (0),
   decrypt (1),
   both    (2)
}
 (encrypt | decrypt | both)

MarkingDataInfo ::= SEQUENCE SIZE(1..MAX) OF MarkingData

MarkingData ::= SEQUENCE {
   markingPhrase  MarkingPhrase  OPTIONAL,
   markingCodes   MarkingCodes  OPTIONAL
}
 (ALL EXCEPT({-- néant; une composante au moins doit être présente --}))

MarkingPhrase ::= DirectoryString { ubMarkingPhraseLength }

MarkingCodes ::= SEQUENCE SIZE(1..MAX) OF MarkingCode

MarkingCode ::= INTEGER {
   pageTop           (1),
   pageBottom        (2),
   pageTopBottom     (3),
   documentEnd       (4),
   noNameDisplay     (5),
   noMarkingDisplay  (6),
   unused            (7),
   documentStart     (8),
   suppressClassName (9)
}

OptionalCategoryGroups ::=
      SEQUENCE SIZE(1..MAX) OF OptionalCategoryGroup
```

```
OptionalCategoryGroup ::= SEQUENCE {
   operation      Operation,
   categoryGroup  CategoryGroup
}

Operation ::= INTEGER {
   onlyOne   (1),
   oneOrMore (2),
   all       (3)
}
 (onlyOne | oneOrMore | all)

CategoryGroup ::= SEQUENCE SIZE(1..MAX) OF OptionalCategoryData

OptionalCategoryData ::= SEQUENCE {
   optCatDataId  OC-DATA.&id({CatData}),
   categorydata  OC-DATA.&Type({CatData}{@optCatDataId })
}

OC-DATA ::= TYPE-IDENTIFIER

CatData OC-DATA ::= {
   ...  -- défini selon les besoins --
}

EquivalentPolicy ::= SEQUENCE {
   securityPolicyId    OBJECT IDENTIFIER,
   securityPolicyName  SecurityPolicyName  OPTIONAL
}

SecurityPolicyName ::= DirectoryString { ubObjectIdNameLength }

clearance ATTRIBUTE ::= {
   WITH SYNTAX  Clearance
   ID           id-at-clearance
}

Clearance ::= SEQUENCE {   -- Etiquettes automatiques appliquées
   policyId            [0] OBJECT IDENTIFIER,
   classList           [1] ClassList  DEFAULT { unclassified },
   securityCategories  [2] SecurityCategories  OPTIONAL
}
```

```
ClassList ::= BIT STRING {
   unmarked     (0),
   unclassified (1),
   restricted   (2),
   confidential (3),
   secret       (4),
   topSecret    (5)
}

-- valeurs des limites supérieures

ubObjectIdNameLength        INTEGER ::= 256
ubClassificationNameLength  INTEGER ::= 256
ubMarkingPhraseLength       INTEGER ::= 256

-- classes d'objets d'information --

ALGORITHM ::= CLASS {
   &id    OBJECT IDENTIFIER  UNIQUE,
   &Type  OPTIONAL
}
  WITH SYNTAX { OID &id [PARMS &Type] }

-- types paramétrisés --

SIGNED { ToBeSigned } ::= SEQUENCE {
   toBeSigned  ToBeSigned,
   algorithm   AlgorithmIdentifier{{SignatureAlgorithms}},
   signature   BIT STRING
}

AlgorithmIdentifier { ALGORITHM:IOSet } ::= SEQUENCE {
   algorithm   ALGORITHM.&id({IOSet}),
   parameters  ALGORITHM.&Type({IOSet}{@algorithm}) OPTIONAL
}

SignatureAlgorithms ALGORITHM ::= {
  ... -- défini selon les besoins --
}

END  -- SecurityInformationObjects --
```

Annexe B

Développement de la syntaxe SECURITY-CATEGORY

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

La classe d'objets d'information **SECURITY-CATEGORY** est définie comme étant la classe intégrée **TYPE-IDENTIFIER**.

```
SECURITY-CATEGORY  ::=  TYPE-IDENTIFIER
```

Cette classe d'objets d'information utiles est spécifiée comme suit à l'Annexe A de la Rec. UIT-T X.681 | ISO/CEI 8824-2:

```
TYPE-IDENTIFIER ::= CLASS {
     &id    OBJECT IDENTIFIER UNIQUE,
     &Type
}
     WITH SYNTAX { &Type IDENTIFIED BY &id }
```

La classe **SECURITY-CATEGORY** a deux champs appelés **&id et &Type**. Le champ **&id** est défini comme étant une valeur de type **OBJECT IDENTIFiER** et le champ **&Type** est un type ouvert. Un type ouvert peut être un type ASN.1 quelconque.

Lorsque des objets de cette classe sont employés comme membres d'un ensemble d'objets d'information, la définition du champ **&id** exige que chaque objet de l'ensemble contienne une valeur d'identificateur d'objet unique. La définition de la classe contient également une déclaration **WITH SYNTAX** qui spécifie une notation pouvant être utilisée pour définir des objets d'information de classe **SECURITY-CATEGORY**.

L'ensemble **SecurityCategoriesTable** est un ensemble d'objets d'information de classe **SECURITY-CATEGORY**. Elle est définie comme suit:

```
SecurityCategoriesTable SECURITY-CATEGORY ::= {
     ...  -- objets définis selon les besoins --
}
```

L'ensemble **SecurityCategoriesTable** contient un marqueur d'extension "..." mais pas d'objets d'information. Les objets de classe **SECURITY-CATEGORY** peuvent être spécifiés individuellement au moyen de la notation **WITH SYNTAX** figurant dans la définition de la classe. Les exemples d'objets suivants montrent que tout type ASN.1, simple ou complexe, peut être employé pour créer un objet d'information.

```
-- Type 1 – attributs restrictifs

restrictiveBitMap SECURITY-CATEGORY ::= {
     AttributeFlags IDENTIFIED BY id-restrictiveBitMap
}

AttributeFlags ::= BIT STRING

-- Type 2 – attributs hiérarchiques

enumeratedAttributes SECURITY-CATEGORY ::= {
     AttributeList IDENTIFIED BY id-enumeratedAttributes
}

AttributeList ::= SET SIZE(1..MAX) OF LabelAttribute

-- Type 5 – tous les attributs dans le ou les domaines

rangeSet SECURITY-CATEGORY ::= {
     RangeList IDENTIFIED BY id-rangeSet
}

RangeList ::= SET SIZE(1..MAX) OF LabelAttributeRange

-- Type 6 – attributs de libération

permissiveBitMap SECURITY-CATEGORY ::= {
     PermissiveBitMap IDENTIFIED BY id-permissiveBitMap

}

PermissiveBitMap ::= BIT STRING
```

```
-- Type 7 - pour le marquage sans contrôle d'accès formel --

freeFormField SECURITY-CATEGORY ::= {
     FreeFormField IDENTIFIED BY id-freeFormField
}

FreeFormField ::= SEQUENCE {
   name   SECURITY-CATEGORY.&id({Fields}),
   field  SECURITY-CATEGORY.&Type({Fields}{@name})
}

Fields SECURITY-CATEGORY ::= {
   ...  -- défini selon les besoins --
}
```

Ici, les champs **&Type** des objets contiennent des types ASN.1 nommés **AttributeFlags**, **AttributeList**, **RangeList**, **PermissiveBitMap** et **FreeFormField**. Les champs **&id** contiennent des valeurs d'identificateurs d'objet uniques nommées **id-restrictiveBitMap**, **id-enumeratedAttributes**, **id-rangeSet**, **id-permissiveBitMap** et **id-freeFormField**.

Ces objets peuvent être ajoutés à une version d'implémentation du tableau **SecurityCategoriesTable** par nom d'objet de manière à former un ensemble de catégories de sécurité à partir de la réunion des objets:

```
SecurityCategoriesTable SECURITY-CATEGORY ::= {
       restrictiveBitMap |
       enumeratedAttributes  |
       rangeSet       |
       permissiveBitMap
       freeFormField,
       ...  -- autres objets attendus --
}
```

A l'inverse, les définitions des objets peuvent directement être ajoutées à l'ensemble d'objets d'information **SecurityCategoriesTable**:

```
SecurityCategoriesTable SECURITY-CATEGORY ::= {
       --
       --    &Type                                  &id
       --
       { AttributeFlags   IDENTIFIED BY id-restrictiveBitMap    } |
       { AttributeList    IDENTIFIED BY id-enumeratedAttributes } |
       { RangeList        IDENTIFIED BY id-rangeSet             } |
       { PermissiveBitMap IDENTIFIED BY id-permissiveBitMap     } |
       { FreeFormField    IDENTIFIED BY id-freeFormField       },
       ...  -- autres objets attendus --
  }
```

Cette conception de l'ensemble des catégories de sécurité fait apparaître un tableau à quatre lignes, chaque ligne comportant deux colonnes, l'une pour **&id** et l'autre pour **&Type**.

Le type **SecurityCategory** est défini comme étant une séquence de deux composantes nommées type et value.

```
SecurityCategory ::= SEQUENCE {
       type   [0] SECURITY-CATEGORY.&id({SecurityCategoriesTable}),
       value  [1] EXPLICIT SECURITY-CATEGORY.&Type(
                           {SecurityCategoriesTable}{@type})
}
```

Chacune des composantes est spécifiée en fonction des champs **&id** and **&Type** de classe **SECURITY-CATEGORY**. La composante **type** est spécifiée en fonction du champ **&id** et doit avoir une valeur de type **OBJECT IDENTIFIER**. La composante value est spécifiée par le champ **&Type** et peut être avoir la valeur d'un type ASN.1 quelconque.

L'ensemble d'objets d'information **SecurityCategoriesTable** est utilisé pour former une contrainte tabulaire sur les valeurs valables des composantes **type** et **value** du type **SecurityCategory**. La contrainte tabulaire est à deux colonnes, une colonne pour chaque champ de la classe **SECURITY-CATEGORY**.

La valeur unique de l'identificateur d'objet spécifiée par le champ **&id** de la composante **type** sélectionne une ligne dans le tableau. La notation **@type** sélectionne la colonne **&Type** associée à la valeur **&id** de la ligne choisie. Le marqueur d'extension dans l'ensemble **SecurityCategoriesTable** indique qu'une application devrait anticiper des objets autres que ceux qui sont spécifiés explicitement dans l'ensemble.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série B	Moyens d'expression: définitions, symboles, classification
Série C	Statistiques générales des télécommunications
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	RGT et maintenance des réseaux: systèmes de transmission, de télégraphie, de télécopie, circuits téléphoniques et circuits loués internationaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données et communication entre systèmes ouverts**
Série Y	Infrastructure mondiale de l'information et protocole Internet
Série Z	Langages et aspects informatiques généraux des systèmes de télécommunication

Genève, 2001