NORME INTERNATIONALE

ISO/CEI 15816

Première édition
2002-02-01

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

Information technology — Security techniques — Security information objects for access control

Numéro de référence
ISO/CEI 15816:2002(F)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax. + 41 22 749 09 47
E-mail copyright@iso.ch
Web www.iso.ch

Imprimé en Suisse

TABLE DES MATIÈRES

Page

1 Domaine d'application 1

2 Références normatives 1

2.1 Recommandations | Normes internationales identiques 1

2.2 Paires de Recommandations | Normes internationales équivalentes par leur contenu technique 2

3 Définitions 2

4 Abréviations 3

5 Conventions 3

5.1 Description de la classe d'objets d'information de sécurité 3

5.2 Correspondance de classe générique d'objets d'information de sécurité 3

5.3 Composition des objets d'information de sécurité 3

6 Spécification des objets d'information de sécurité 3

6.1 Etiquettes de confidentialité 4

6.1.1 Introduction 4

6.1.2 Spécification ASN.1 de l'étiquette 4

6.1.3 Méthode d'établissement de lien pour les étiquettes de confidentialité 5

6.2 Fichier d'information sur la politique de sécurité 6

6.2.1 Introduction 6

6.2.2 Spécification ASN.1 du fichier d'information sur la politique de sécurité 6

6.3 Attribut clearance (autorisation) 10

6.3.1 Introduction 10

6.3.2 Définition de l'attribut clearance 11

7 Interaction des objets d'information de sécurité 11

7.1 Comparaison de la structure de classe des objets SIO 11

7.2 Interaction des objets d'information de sécurité pour le contrôle d'accès 11

Annexe A – Objets d'information de sécurité pour le contrôle d'accès en ASN.1 14

Annexe B – Développement de la syntaxe **SECURITY-CATEGORY** 20

Avant-propos

L'ISO (Organisation internationale de normalisation) et la CEI (Commission électrotechnique internationale) forment le système spécialisé de la normalisation mondiale. Les organismes nationaux membres de l'ISO ou de la CEI participent au développement de Normes internationales par l'intermédiaire des comités techniques créés par l'organisation concernée afin de s'occuper des domaines particuliers de l'activité technique. Les comités techniques de l'ISO et de la CEI collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO et la CEI participent également aux travaux. Dans le domaine des technologies de l'information, l'ISO et la CEI ont créé un comité technique mixte, l'ISO/CEI JTC 1.

Les Normes internationales sont rédigées conformément aux règles données dans les Directives ISO/CEI, Partie 3.

La tâche principale du comité technique mixte est d'élaborer les Normes internationales. Les projets de Normes internationales adoptés par le comité technique mixte sont soumis aux organismes nationaux pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des organismes nationaux votants.

L'attention est appelée sur le fait que certains des éléments de la présente Norme internationale peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO et la CEI ne sauraient être tenues pour responsables de ne pas avoir identifié de tels droits de propriété et averti de leur existence.

L'ISO/CEI 15816 a été élaborée par le comité technique mixte ISO/CEI JTC 1, *Technologies de l'nformation*, sous-comité SC 27, *Techniques de sécurité des technologies de l'information*, en collaboration avec l'UIT-T. Le texte identique est publié en tant que Rec. UIT-T X.841.

L'annexe A constitue un élément normatif de la présente Norme internationale. L'annexe B est donnée uniquement à titre d'information.

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-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.