NORME INTERNATIONALE ISO/CEI 10164-9:1995
RECTIFICATIF TECHNIQUE 2

Publié 1999-11-01

Version française parue en 2000

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION
INTERNATIONAL ELECTROTECHNICAL COMMISSION • МЕЖДУНАРОДНАЯ ЭЛЕКТРОТЕХНИЧЕСКАЯ КОМИССИЯ • COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

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

RECTIFICATIF TECHNIQUE 2

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

TECHNICAL CORRIGENDUM 2

Le Rectificatif technique 2 à la Norme internationale ISO/CEI 10164-9:1995 a été élaboré par le comité technique mixte ISO/CEI JTC 1, *Technologies de l'information*.

ICS 35.100.70 **Réf. nº ISO/CEI 10164-9:1995/Cor.2:1999(F)**

Imprimé en Suisse

Page blanche

NORME INTERNATIONALE

RECOMMANDATION UIT-T

TECHNOLOGIES DE L'INFORMATION – INTERCONNEXION DES SYSTÈMES OUVERTS – GESTION DES SYSTÈMES: OBJETS ET ATTRIBUTS POUR LE CONTRÔLE D'ACCÈS

CORRIGENDUM TECHNIQUE 2

1) Paragraphe A.2.3

Remplacer **AccessControl-ASN1Module.denyAccess** *par* **AccessControl-ASN1Module.deny**

Supprimer le **PRESENT IF** *(formaté en blanc et donc non visible sur l'exemplaire imprimé) des spécifications* **CONDITIONAL PACKAGE** *pour* **duration**, **dailyScheduling**, **weeklyScheduling** *et* **externalScheduler**

Dans la production **authenticationContextPackage** *remplacer*

REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) package(4) (2) }; *par*

REGISTERED AS { joint-iso-ccitt(2) ms(9) function(2) part9(9) package(4) authenticationContextPackage(2) };

2) Paragraphe A.2.4

A la fin de **accessControlNotificationEmitterPkg** *remplacer* **;;;** *par* **;;;;**

3) Paragraphe A.2.5

Dans **operationsListPackage ATTRIBUTES operationsList**

remplacer **ADD-REMOVE;;** *par* **ADD-REMOVE;**

Dans **operationsListPackage REGISTERED AS**

remplacer **(15)}** *par* **(15)};**

Dans **operationsListPackage PRESENT IF**

remplacer **contenu !** *par* **contenu!;**

4) Paragraphe A.2.11

Remplacer **DERIVED FROM top** *par* **DERIVED FROM "CCITT Rec. X.721 | ISO/IEC 10165-2:1992":top**

5) Paragraphe A.2.14

Ne concerne que la version anglaise.

6) Paragraphe A.4.1

Remplacer **AccessControlDefinitions** *par* **AccessControl-ASN1Module**

7) Paragraphe A.5.1

Remplacer **AccessControlDefinitions** *par* **AccessControl-ASN1Module**

8) Paragraphe A.5.2

Remplacer **AccessControlDefinitions** *par* **AccessControl-ASN1Module**

9) Paragraphe A.5.3

Remplacer **AccessControlDefinitions** *par* **AccessControl-ASN1Module**

10) Paragraphe A.5.4

Remplacer **AccessControlDefinitions** *par* **AccessControl-ASN1Module**

Remplacer **PARAMETERS invalidAccesscontrolFilter** *par* **PARAMETERS invalidAccessControlFilter**

11) Paragraphe A.5.6

Remplacer **AccessControlDefinitions** *par* **AccessControl-ASN1Module**

12) Paragraphe A.5.7

Remplacer **AccessControlDefinitions** *par* **AccessControl-ASN1Module**

13) Paragraphe A.5.8

Remplacer **AccessControlDefinitions** *par* **AccessControl-ASN1Module**

14) Paragraphe A.5.9

Remplacer **AccessControlDefinitions** *par* **AccessControl-ASN1Module**

15) Paragraphe A.5.10

Remplacer **AccessControlDefinitions** *par* **AccessControl-ASN1Module**

16) Paragraphe A.5.11

Remplacer **AccessControlDefinitions** *par* **AccessControl-ASN1Module**

17) Paragraphe A.5.12

Remplacer **AccessControlDefinitions** *par* **AccessControl-ASN1Module**

18) Paragraphe A.5.14

Remplacer **AccessControlDefinitions** *par* **AccessControl-ASN1Module**

19) Paragraphe A.5.17

Remplacer **AccessControlDefinitions** *par* **AccessControl-ASN1Module**

20) Paragraphe A.5.18

Remplacer **AccessControlDefinitions** *par* **AccessControl-ASN1Module**

Remplacer **EQUALITY SET-COMPARISON** *par* **EQUALITY, SET-COMPARISON**

21) Paragraphe A.5.20

Remplacer **AccessControlDefinitions** *par* **AccessControl-ASN1Module**

22) Paragraphe A.5.21

Remplacer **AccessControlDefinitions** *par* **AccessControl-ASN1Module**

23) Paragraphe A.5.22

Remplacer **AccessControlDefinitions** *par* **AccessControl-ASN1Module**

24) Paragraphe A.5.24

Remplacer **AccessControlDefinitions** *par* **AccessControl-ASN1Module**

25) Paragraphe A.5.25

Remplacer **AccessControlDefinitions** *par* **AccessControl-ASN1Module**

26) Paragraphe A.5.26

Remplacer **AccessControlDefinitions** *par* **AccessControl-ASN1Module**

27) Paragraphe A.6

Dans la première ligne:

remplacer **AccessControlDefinitions { joint-iso-ccitt ms(9) function(2) part9(9) asn1Module(2) 1 }**

par **AccessControl-ASN1Module { joint-iso-ccitt ms(9) function(2) part9(9) asn1Module(2) 2 }**

Avant le **IMPORTS** *pour* **DistinguishedName** *ajouter la Note suivante sous forme de commentaire ASN.1:*

```
-- NOTE – La présente Recommandation | Norme internationale importe les noms distinctifs de la
-- Rec. X.501 du CCITT (1988) | ISO/CEI 9594-2:1990. La spécification de cette syntaxe peut maintenant
-- être consultée dans une annexe informative de la Rec. UIT-T X.711 (1997) | ISO/CEI 9596-1:1997.
```

Supprimer ce qui suit:

```
FunctionalUnitPackage
    FROM SMASE-A-ASSOCIATE-Information { joint-iso-ccitt ms(9) smo(0) negotiationAbstractSyntax(1) version1(1) }
```

Remplacer le **IMPORTS** *pour* **AETitle** *par ce qui suit:*

AE-title
FROM ACSE-1 { joint-iso-itu-t(2) association-control(2) modules(0) apdus(0) version1(1) }

Dans **InitiatorName** *remplacer* **InitiatorName CHOICE** *par* **InitiatorName ::= CHOICE**

Dans **InitiatorName** *remplacer* **[4] IMPLICIT AETitle** *par* **[4] AE-title**

Dans **CapabilityIdentitiesList** *remplacer* **IMPLICIT OBJECT IDENTIFIER** *par* **OBJECT IDENTIFIER**

Dans **DenialResponse** *supprimer* **EnforcementAction**

Dans **Deny** *remplacer* **Deny** *par* **deny**

Dans **InvalidAccessControlFilter** *supprimer le* { *(formaté en blanc et donc non visible sur l'exemplaire imprimé) avant* **filter**

Page blanche

Page blanche

NORME INTERNATIONALE

ISO/CEI 10164-9

Première édition
1995-12-15

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

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

Numéro de référence
ISO/CEI 10164-9:1995(F)

Sommaire

Version française tirée en 1996

Imprimé en Suisse

Avant-propos

L'ISO (Organisation internationale de normalisation) et la CEI (Commission électrotechnique internationale) forment ensemble un système consacré à la normalisation internationale considérée comme un tout. Les organismes nationaux membres de l'ISO ou de la CEI participent au développement de Normes internationales par l'intermédiaire des comités techniques créés par l'organisation concernée afin de s'occuper des différents domaines particuliers de l'activité technique. Les comités techniques de l'ISO et de la CEI collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales ou non gouvernementales, en liaison avec l'ISO et la CEI participent également aux travaux.

Dans le domaine des technologies de l'information, l'ISO et la CEI ont créé un comité technique mixte, l'ISO/CEI JTC 1. Les projets de Normes internationales adoptés par le comité technique mixte sont soumis aux organismes nationaux pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des organismes nationaux votants.

La Norme internationale ISO/CEI 10164-9 a été élaborée par le comité technique mixte ISO/CEI JTC 1, *Technologies de l'information*, sous-comité SC 21, *Interconnexion des systèmes ouverts, gestion des données et traitement distribué ouvert*, en collaboration avec l'UIT-T. Le texte identique est publié en tant que Recommandation UIT-T X.741.

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

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

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

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

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

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

— *Partie 6: Fonction de contrôle de journal*

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

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

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

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

— *Partie 11: Objets et attributs métriques*

— *Partie 12: Fonction de gestion des tests*

— *Partie 13: Fonction de récapitulation*

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

— *Partie 15: Fonction de programmation*

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

— *Partie 17: Fonction de changement*

— *Partie 18: Fonction de gestion de logiciel*

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

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

Introduction

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

Page blanche

NORME INTERNATIONALE

RECOMMANDATION UIT-T

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

1 Domaine d'application

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

La présente Recommandation | Norme internationale:

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

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

La présente Recommandation | Norme internationale:

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