



UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

CCITT

COMITÉ CONSULTATIF
INTERNATIONAL
TÉLÉGRAPHIQUE ET TÉLÉPHONIQUE

X.740

(09/92)

**RÉSEAUX DE COMMUNICATIONS
DE DONNÉES**

**TECHNOLOGIE DE L'INFORMATION –
INTERCONNEXION DE SYSTÈMES
OUVERTS – GESTION DES SYSTÈMES:
FONCTION DE PISTE DE VÉRIFICATION
DE SÉCURITÉ**



Recommandation X.740

Avant-propos

L'UIT (Union internationale des télécommunications) est une institution spécialisée des Nations Unies dans le domaine des télécommunications. Le CCITT (Comité consultatif international télégraphique et téléphonique) est un organe permanent de l'UIT. Au sein du CCITT, qui est l'entité qui établit les normes mondiales (Recommandations) sur les télécommunications, participent quelque 166 pays membres, 68 exploitations privées reconnues, 163 organisations scientifiques et industrielles et 39 organisations internationales.

L'approbation des Recommandations par les membres du CCITT s'effectue selon la procédure définie dans la Résolution n° 2 du CCITT (Melbourne, 1988). De plus, l'Assemblée plénière du CCITT, qui se réunit tous les quatre ans, approuve les Recommandations qui lui sont soumises et établit le programme d'études pour la période suivante.

Dans certains secteurs de la technologie de l'information qui correspondent à la sphère de compétence du CCITT, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI. Le texte de la Recommandation X.740 du CCITT a été approuvé le 10 septembre 1992. Son texte est publié, sous forme identique, comme Norme internationale ISO/CEI 10164-8.

NOTE DU CCITT

Dans cette Recommandation, l'expression «Administration» est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation privée reconnue.

© UIT 1993

Droits de reproduction réservés. Aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'UIT.

Table des matières

Page

1	Champ d'application.....	1
2	Références normatives	1
2.1	Recommandations Normes internationales identiques.....	2
2.2	Paires de Recommandations Normes internationales équivalentes par leur contenu technique	2
2.3	Références additionnelles	3
3	Définitions.....	3
3.1	Définitions du modèle de référence de base	3
3.2	Définitions de l'architecture de sécurité	3
3.3	Définitions du cadre de gestion.....	3
3.4	Définitions de l'aperçu général de la gestion de systèmes	4
3.5	Définitions de la gestion des rapports d'événement	4
3.6	Définitions du rapport d'alarme sécurité	4
3.7	Définitions de la commande des registres de consignation.....	4
3.8	Définitions du test de conformité OSI	4
4	Abréviations	4
5	Conventions.....	5
6	Spécifications	5
7	Modèle.....	6
8	Définitions génériques	6
8.1	Notifications génériques	6
8.2	Objet géré.....	7
8.3	Définitions génériques importées.....	7
8.4	Conformité	7
9	Définition du service	8
9.1	Introduction.....	8
9.2	Service rapport de piste de vérification de sécurité	8
10	Unités fonctionnelles.....	9
11	Protocole	9
11.1	Eléments de procédure	9
11.2	Syntaxe abstraite	9
11.3	Négociation des unités fonctionnelles de rapport de piste de vérification de sécurité	11
12	Relations avec d'autres fonctions	11
13	Conformité	11
13.1	Spécifications de la classe de conformité générale	11
13.2	Spécifications de la classe de conformité induite.....	12
13.3	Spécifications de la conformité de l'information de gestion	12
13.4	Spécifications du PICS	12
Annexe A	Définition de l'information de gestion	13
Annexe B	Formulaire MCS	15
Annexe C	Formulaire MOCS	17
Annexe D	Formulaire MIDS (notification).....	20
Annexe E	Formulaire PICS	21
Annexe F	Relation avec le cadre de vérification de sécurité	27

NOTE D'INFORMATION

Le tableau suivant indique une liste de Recommandations de la série X.700 élaborées en collaboration avec l'ISO/CEI et qui sont identiques à la Norme internationale correspondante. Ce tableau mentionne les références aux numéros des Normes internationales ISO/CEI ainsi que le titre abrégé de la Recommandation | Norme internationale.

Recommandation du CCITT Norme internationale ISO/CEI	Titre abrégé
X.700 7498-4 (remarque)	Cadre de gestion
X.701 10040	Aperçu général de la gestion des systèmes
X.710 9595 (remarque)	Définition du service commun de transfert d'informations de gestion
X.711 9596-1 (remarque)	Spécification du protocole commun de transfert d'informations de gestion
X.712 9596-2	CMIP PICS
X.720 10165-1	Modèle d'information de gestion
X.721 10165-2	Définition des informations de gestion
X.722 10165-4	Directives pour la définition des objets gérés
X.730 10164-1	Fonction de gestion des objets
X.731 10164-2	Fonction de gestion d'états
X.732 10164-3	Attributs pour représenter les relations
X.733 10164-4	Fonction de signalisation des alarmes
X.734 10164-5	Fonction de gestion des rapports d'événement
X.735 10164-6	Fonction de commande des registres de consignation
X.736 10164-7	Fonction de signalisation des alarmes de sécurité
X.740 10164-8	Fonction de piste de vérification de sécurité
REMARQUE – Cette Recommandation et la Norme internationale ne sont pas identiques, par contre elles sont alignées au point de vue technique.	

NORME INTERNATIONALE

RECOMMANDATION DU CCITT

TECHNOLOGIE DE L'INFORMATION – INTERCONNEXION DE SYSTÈMES OUVERTS – GESTION DES SYSTÈMES: FONCTION DE PISTE DE VÉRIFICATION DE SÉCURITÉ

1 Champ d'application

La présente Recommandation | Norme internationale définit la fonction de piste de vérification de sécurité. Il s'agit d'une fonction de gestion des systèmes qui peut être utilisée par un processus d'application dans un environnement de gestion centralisée ou décentralisée afin d'échanger les informations et commandes de gestion des systèmes, telle qu'elle est définie dans la Rec. X.700 du CCITT | ISO/CEI 7498-4. La présente Recommandation | Norme internationale se situe dans la couche application de la Rec. X.200 du CCITT | ISO 7498; elle est définie conformément au modèle fourni par ISO/CEI 9545. Le rôle des fonctions de gestion des systèmes est décrit dans la Rec. X.701 du CCITT | ISO/CEI 10040.

La présente Recommandation | Norme internationale:

- établit les spécifications usager pour la définition du service nécessaire pour assurer la fonction de rapport de piste de vérification de sécurité;
- définit le service fourni par la fonction de rapport de piste de vérification de sécurité;
- spécifie le protocole nécessaire à la fourniture du service;
- définit les relations entre le service et les notifications de gestion;
- définit les relations avec d'autres fonctions de gestion des systèmes;
- spécifie les conditions de conformité.

En revanche, la présente Recommandation | Norme internationale ne définit pas:

- de vérification de sécurité, ni la manière d'en effectuer une. Une vérification de sécurité peut être utilisée pour évaluer l'efficacité d'une politique de sécurité. La politique de sécurité identifie les catégories des événements liés à la sécurité qui nécessitent une vérification, ainsi que l'emplacement du registre de piste de vérification de sécurité dans lequel ces événements doivent être enregistrés;
- la nature d'une quelconque mise en œuvre destinée à assurer la fonction de piste de vérification de sécurité;
- les circonstances dans lesquelles l'utilisation de la fonction de piste de vérification de sécurité est appropriée;
- les services nécessaires à l'établissement et à la libération normale ou anormale d'une association de gestion;
- d'autres notifications définies dans d'autres Recommandations | Normes internationales qui peuvent intéresser l'administrateur de sécurité.

2 Références normatives

Les Recommandations du CCITT 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. Toute Recommandation et

Norme 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 Secrétariat du CCITT tient à jour une liste des Recommandations du CCITT actuellement en vigueur.

2.1 Recommandations | Normes internationales identiques

- Recommandation X.701 du CCITT (1992) | ISO/CEI 10040:1992, *Technologies de l'information – Interconnexion de systèmes ouverts – Aperçu général de la gestion des systèmes.*
- Recommandation X.721 du CCITT (1992) | ISO/CEI 10165-2:1992, *Technologies de l'information – Interconnexion de systèmes ouverts – Structure des informations de gestion – Définition des informations de gestion.*
- Recommandation X.722 du CCITT (1992) | ISO/CEI 10165-4:1992, *Technologies de l'information – Interconnexion de systèmes ouverts – Structure des informations de gestion – Directives pour la définition des objets gérés.*
- Recommandation X.724¹⁾ du CCITT | ISO/CEI 10165-6¹⁾, *Technologies de l'information – Interconnexion de systèmes ouverts – Structure de l'information de gestion: exigences et directives pour les modèles de déclaration de conformité d'une mise en œuvre associés à l'information de gestion.*
- Recommandation X.733 du CCITT (1992) | ISO/CEI 10164-4:1992, *Technologies de l'information – Interconnexion de systèmes ouverts – Gestion des systèmes – Fonction de rapport d'alarme.*
- Recommandation X.734 du CCITT (1992) | ISO/CEI 10164-5:1993, *Technologies de l'information – Interconnexion de systèmes ouverts – Gestion des systèmes – Fonction de gestion des rapports d'événements.*
- Recommandation X.735 du CCITT (1992) | ISO/CEI 10164-6:1993, *Technologies de l'information – Interconnexion de systèmes ouverts – Gestion des systèmes – Fonction de gestion des registres de consignment.*
- Recommandation X.736 du CCITT (1992) | ISO/CEI 10164-7:1992, *Technologies de l'information – Interconnexion de systèmes ouverts – Gestion des systèmes – Fonction de signalisation des alarmes de sécurité.*

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

- Recommandation X.200 du CCITT (1988), *Modèle de référence pour l'interconnexion des systèmes ouverts pour les applications du CCITT.*
ISO 7498:1984, *Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Modèle de référence de base.*
- Recommandation X.208 du CCITT (1988), *Spécification de la syntaxe abstraite numéro un (ASN.1).*
ISO/CEI 8824:1990, *Technologies de l'information – Interconnexion de systèmes ouverts – Spécification de la notation de syntaxe abstraite numéro un (ASN.1).*
- Recommandation X.209 du CCITT (1988), *Spécification des règles de codage pour la notation de syntaxe abstraite numéro un (ASN.1).*
ISO/CEI 8825:1990, *Technologies de l'information – Interconnexion de systèmes ouverts – Spécification de règles de base pour coder la notation de syntaxe abstraite numéro un (ASN.1).*
- Recommandation X.210 du CCITT (1988), *Conventions relatives à la définition de service des couches de l'interconnexion de systèmes ouverts.*
ISO/TR 8509:1987, *Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Conventions de service.*
- Recommandation X.290 du CCITT (1992), *Cadre général et méthodologie des tests de conformité OSI pour les Recommandations sur les protocoles pour les applications du CCITT – Concepts généraux.*

¹⁾ Actuellement à l'état de projet.

ISO/CEI 9646-1:1991, *Technologies de l'information – Interconnexion de systèmes ouverts – Cadre général et méthodologie des tests de conformité – Partie 1: Concepts généraux.*

- Recommandation X.291 du CCITT (1992), *Cadre général et méthodologie des tests de conformité OSI pour les Recommandations sur les protocoles pour les applications du CCITT – Spécification des suites de tests abstraites.*

ISO/CEI 9646-2:1991, *Technologies de l'information – Interconnexion de systèmes ouverts – Cadre général et méthodologie des tests de conformité – Partie 2: Spécification des suites de tests abstraites.*

- Recommandation X.700 du CCITT (1992), *Définition du cadre de gestion pour l'interconnexion de systèmes ouverts (OSI) pour les applications du CCITT.*

ISO/CEI 7498-4:1989, *Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Modèle de référence de base – Partie 4: Cadre général de gestion.*

- Recommandation X.710 du CCITT (1991), *Définition du service commun de transfert d'informations de gestion pour les applications du CCITT.*

ISO/CEI 9595:1991, *Technologies de l'information – Interconnexion de systèmes ouverts – Définition du service commun d'informations de gestion.*

- Recommandation X.800 du CCITT (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.*

2.3 Références additionnelles

- ISO/CEI 9545:1989, *Technologies de l'information – Interconnexion de systèmes ouverts – Structure de la Couche Application.*
- ISO/CEI 10181-7²⁾, *Technologies de l'information – Interconnexion de systèmes ouverts – Cadres de sécurité – Partie 7: Cadre de vérification de sécurité.*

3 Définitions

Les définitions suivantes s'appliquent dans le cadre de la présente Recommandation | Norme internationale.

3.1 Définitions du modèle de référence de base

La présente Recommandation | Norme internationale utilise le terme suivant défini dans la Rec. X.200 du CCITT | ISO 7498:

système ouvert.

3.2 Définitions de l'architecture de sécurité

La présente Recommandation | Norme internationale utilise les termes suivants définis dans la Rec. X.800 du CCITT | ISO 7498-2:

- a) piste de vérification de sécurité;
- b) politique de sécurité.

3.3 Définitions du cadre de gestion

La présente Recommandation | Norme internationale utilise le terme suivant défini dans la Rec. X.700 du CCITT | ISO/CEI 7498-4:

objet géré.

²⁾ Actuellement à l'état de projet.

3.4 Définitions de l'aperçu général de la gestion de systèmes

La présente Recommandation | Norme internationale utilise les termes suivants définis dans la Rec. X.701 du CCITT | ISO/CEI 10040:

- a) rôle d'agent;
- b) conformité induite;
- c) conformité générale;
- d) domaine de gestion;
- e) rôle de gestionnaire;
- f) notification;
- g) unité fonctionnelle de gestion des systèmes.

3.5 Définitions de la gestion des rapports d'événement

La présente Recommandation | Norme internationale utilise le terme suivant défini dans la Rec. X.734 du CCITT | ISO/CEI 10164-5:

discriminateur.

3.6 Définitions du rapport d'alarme sécurité

La présente Recommandation | Norme internationale utilise le terme suivant défini dans la Rec. X.736 du CCITT | ISO/CEI 10164-7:

événement relatif à la sécurité.

3.7 Définitions de la commande des registres de consignation

La présente Recommandation | Norme internationale utilise les termes suivants définis dans la Rec. X.735 du CCITT | ISO/CEI 10164-6:

- a) registre de consignation;
- b) enregistrement de consignation.

3.8 Définitions du test de conformité OSI

La présente Recommandation | Norme internationale utilise les termes suivants définis dans la Rec. X.290 du CCITT | ISO/CEI 9646-1:

- a) formulaire PICS;
- b) déclaration de conformité d'une instance de protocole (PICS);
- c) déclaration de conformité d'un système.

4 Abréviations

ASN.1	Notation de syntaxe abstraite numéro un (<i>abstract syntax notation one</i>)
CMIS	Service commun d'information de gestion (<i>common management information service</i>)
Conf	Confirmation
Ind	Indication
MAPDU	Unité de données du protocole d'application de gestion (<i>management application protocol data unit</i>)
MCS	Résumé de conformité de gestion (<i>management conformance summary</i>)
MIDS	Déclaration de définition d'information de gestion (<i>management information definition statement</i>)

MOCS	Déclaration de conformité d'objet géré (<i>managed object conformance statement</i>)
OSI	Interconnexion de systèmes ouverts (<i>open systems interconnection</i>)
PICS	Déclaration de conformité d'une instance de protocole (<i>protocol implementation conformance statement</i>)
Req	Demande (<i>request</i>)
Rsp	Réponse (<i>response</i>)
SMAPM	Machine protocole d'application de gestion des systèmes (<i>systems management application protocol machine</i>)

5 Conventions

La présente Recommandation | Norme internationale définit les services pour la fonction de piste de vérification de sécurité conformément aux conventions descriptives définies dans la Rec. X.210 du CCITT | ISO/TR 8509. Dans l'article 9, la définition de chaque service contient un tableau énumérant les paramètres de ses primitives. Pour une primitive donnée, la présence de chaque paramètre est décrite par l'une des valeurs suivantes:

- O Paramètre obligatoire;
- (=) La valeur de ce paramètre est égale à celle du paramètre de la colonne de gauche;
- U L'utilisation de ce paramètre est une option proposée à l'utilisateur du service;
- Paramètre non présent dans l'interaction décrite par la primitive en question;
- C Paramètre conditionnel. La (les) condition(s) est (sont) définie(s) dans le texte qui décrit le paramètre;
- P Paramètre soumis aux contraintes imposées par la Rec. X.710 du CCITT | ISO/CEI 9595.

REMARQUE – Les paramètres marqués avec «P» dans le tableau 1 sont mis en correspondance directe avec les paramètres correspondants de la primitive de service CMIS, sans modifications sémantiques ou syntaxiques des paramètres. Les autres paramètres sont utilisés pour préparer une MAPDU.

6 Spécifications

L'utilisateur de la gestion de sécurité requiert la possibilité d'enregistrer dans un registre de consignation de piste de vérification de sécurité les événements relatifs à la sécurité qui se produisent dans le domaine de gestion. La politique de sécurité d'un système ouvert peut nécessiter l'envoi des événements particuliers relatifs à la sécurité vers un registre de piste de vérification de sécurité qui se trouve dans le même système ou dans un système ouvert différent.

Parmi les types d'événements relatifs à la sécurité, pouvant faire l'objet de vérification de sécurité, figurent les types suivants (sans être exhaustifs):

- connexions;
- déconnexions;
- utilisation des mécanismes de sécurité;
- opérations de gestion; et
- comptage d'utilisation.

L'utilisateur de la gestion de sécurité requiert également la possibilité de commander le mécanisme de consignation de piste de vérification de sécurité.

La présente Recommandation | Norme internationale décrit l'utilisation des services et mécanismes pour satisfaire ces spécifications.

7 Modèle

La présente Recommandation | Norme internationale requiert que les événements relatifs à la sécurité soient consignés conformément aux procédures définies dans la Rec. X.735 du CCITT | ISO/CEI 10164-6. La construction de discriminateur à l'intérieur de la consignation de piste de vérification de sécurité doit être spécifiée de manière à permettre la saisie des événements entrants dont la politique de sécurité exige la consignation. Si les rapports d'événement doivent être envoyés vers une destination différente, il faut créer les discriminateurs de retransmission d'événement comme les définit la Rec. X.734 du CCITT | ISO/CEI 10164-5 et positionner l'adresse de destination pour transmettre l'événement au système dans lequel se trouve le registre de consignation de piste de vérification de sécurité choisi. Le registre de consignation de piste de vérification de sécurité est un registre conforme à la définition donnée dans la Rec. X.735 du CCITT | ISO/CEI 10164-6.

Le modèle utilisé pour transporter les rapports d'événement vers le système dans lequel se trouve le registre de piste de vérification de sécurité est défini dans la Rec. X.734 du CCITT | ISO/CEI 10164-5. Le modèle de création et d'extraction des entrées dans le registre de piste de vérification de sécurité est défini dans la Rec. X.735 du CCITT | ISO/CEI 10164-6.

8 Définitions génériques

8.1 Notifications génériques

La présente Recommandation | Norme internationale définit un ensemble de notifications génériques de piste de vérification de sécurité avec leurs paramètres et sémantiques applicables.

L'ensemble des notifications génériques, paramètres et sémantiques définis dans la présente Recommandation | Norme internationale fournit les détails relatifs aux paramètres suivants du service G-RAPPORT-ÉVÉNEMENT (M-EVENT-REPORT) tel qu'il est défini dans la Rec. X.710 du CCITT | ISO/CEI 9595:

- type d'événement;
- information relative à l'événement;
- réponse à l'événement.

Toutes les notifications sont des entrées potentielles dans un registre de consignation de la gestion des systèmes. La Rec. X.721 du CCITT | ISO/CEI 10165-2 définit une classe d'objets générique d'enregistrements de consignation d'événements, à partir de laquelle on peut dériver toutes les entrées, les informations additionnelles étant spécifiées dans les paramètres information d'événement et réponse à un événement.

8.1.1 Type d'événement

Ce paramètre définit le type du rapport de piste de vérification de sécurité. La présente Recommandation | Norme internationale définit les types d'événements suivants:

- rapport de service: il s'agit de l'indication d'un événement relatif à la fourniture, au refus ou à la reprise du service. Les causes spécifiques entraînant la génération de cet événement sont décrites en 8.1.2;
- rapport d'utilisation: il s'agit de l'indication d'un enregistrement contenant des informations de nature statistique significatives pour la sécurité.

Il est possible d'enregistrer dans le registre de piste de vérification de sécurité d'autres notifications définies dans d'autres Recommandations | Normes internationales (par exemple, la Rec. X.736 du CCITT | ISO/CEI 10164-7). Les types de notification (analogues aux types de rapport de piste de vérification de sécurité) ainsi que leurs paramètres associés sont définis dans les Recommandations | Normes internationales appropriées.

8.1.2 Information relative à l'événement

Le paramètre cause de rapport de service constitue la notification d'information relative à l'événement spécifique.

Ce paramètre doit être offert lorsque le type d'événement spécifie un rapport de service. Ce paramètre donne des détails supplémentaires concernant la cause probable du rapport de service. La valeur de ce paramètre, prise en considération avec la valeur du type d'événement, détermine les paramètres constituant le rapport de service et les valeurs possibles de ces paramètres.

Les valeurs de cause de rapport de service pour les notifications doivent être indiquées dans l'article relatif au comportement de la définition de la classe d'objet géré. La présente Recommandation | Norme internationale définit des causes de rapport de service ayant de larges applications à travers les classes d'objet géré, pour les utiliser dans le contexte d'application de la gestion des systèmes défini dans la Rec. X.701 du CCITT | ISO/CEI 10040. Ces valeurs sont enregistrées dans l'annexe A à la présente Recommandation | Norme internationale. La syntaxe des causes de rapport de service doit être celle du type identificateur d'objet de l'ASN.1. Des causes de rapport de service supplémentaires, destinées à être utilisées dans le contexte d'application de la gestion des systèmes défini dans la Rec. X.701 du CCITT | ISO/CEI 10040, peuvent être ajoutées à la présente Recommandation | Norme internationale et enregistrées en utilisant les procédures d'enregistrement définies dans la Rec. X.208 du CCITT | ISO/CEI 8824 pour les valeurs d'identificateur d'objet de l'ASN.1.

D'autres causes de rapport de service, destinées à être utilisées dans le contexte d'application de la gestion des systèmes défini dans la Rec. X.701 du CCITT | ISO/CEI 10040, peuvent être définies hors du cadre de la présente Recommandation | Norme internationale et enregistrées en utilisant les procédures d'enregistrement définies dans la Rec. X.208 du CCITT | ISO/CEI 8824 pour les valeurs d'identificateur d'objet de l'ASN.1.

On définit les valeurs suivantes de cause de rapport de service:

- demande de service: cette valeur spécifie le fait que la notification a été générée en raison d'une demande de fourniture d'un service;
- refus de service: cette valeur spécifie le fait que la notification a été générée en raison du refus d'une demande de service;
- réponse de service: cette valeur spécifie le fait que la notification a été générée suite à la satisfaction d'une demande de service;
- défaillance de service: cette valeur spécifie le fait que la notification a été générée suite à la détection pendant la fourniture du service d'une situation anormale qui a entraîné la défaillance du service;
- reprise de service: cette valeur spécifie le fait que la notification a été générée suite au rétablissement du service à partir d'une situation anormale;
- autre raison: cette valeur spécifie le fait que la notification a été générée pour des raisons différentes de celles énumérées ci-dessus. La raison réelle, ainsi que d'autres informations pertinentes, sont spécifiées dans les autres paramètres du rapport.

8.1.3 Réponse à l'événement

La présente Recommandation | Norme internationale ne spécifie pas d'information de gestion destinée à être utilisée dans le paramètre de réponse à l'événement.

8.2 Objet géré

L'enregistrement de piste de vérification de sécurité est une classe d'objet géré dérivée de la classe d'objet enregistrement de consignation d'événement définie dans la Rec. X.721 du CCITT | ISO/CEI 10165-2. La classe d'objet enregistrement de piste de vérification de sécurité représente les informations consignées suite aux notifications de piste de vérification de sécurité.

8.3 Définitions génériques importées

On utilise également les paramètres suivants qui sont définis dans la Rec. X.733 du CCITT | ISO/CEI 10164-4:

- informations additionnelles;
- texte additionnel;
- notifications corrélées;
- identificateur de notification.

8.4 Conformité

Les définitions de classe d'objet géré assurent les fonctions définies dans la présente Recommandation | Norme internationale en incorporant la spécification des notifications par référence aux modèles de notification définis dans l'annexe A. Le mécanisme de référence est défini dans la Rec. X.722 du CCITT | ISO/CEI 10165-4.

Pour chaque occurrence de rapport de piste de vérification de sécurité, il est nécessaire de définir une classe d'objet géré qui importe une ou plusieurs des notifications définies dans la présente Recommandation | Norme internationale afin de sélectionner le type de rapport de piste de vérification de sécurité qui reflète le mieux l'événement réel qui mène à l'objet géré émettant la notification. Pour chaque notification importée, la définition de la classe d'objet géré doit spécifier dans la partie de comportement les paramètres à utiliser parmi les paramètres facultatifs ou conditionnels, les conditions de leur utilisation et leurs valeurs. Il est permis de déclarer que l'utilisation d'un certain paramètre reste facultative.

9 Définition du service

9.1 Introduction

Les notifications de piste de vérification de sécurité fournissent la possibilité de signaler les événements relatifs à la sécurité détectés par un objet géré. Les paramètres acheminent les informations pertinentes concernant la piste de vérification de sécurité.

9.2 Service rapport de piste de vérification de sécurité

Le service rapport de piste de vérification de sécurité utilise les paramètres définis dans l'article 8 de la présente Recommandation | Norme internationale en plus des paramètres du service général G-RAPPORT-ÉVÉNEMENT (M-EVENT-REPORT) défini dans la Rec. X.710 du CCITT | ISO/CEI 9595. Le tableau 1 énumère les paramètres du service rapport de piste de vérification de sécurité.

Tableau 1 – Paramètres de rapport de piste de vérification de sécurité

Nom du paramètre	Demande/Indication	Réponse/Confirmation
Identificateur d'invocation	P	P
Mode	P	–
Classe d'objet géré	P	P
Instance d'objet géré	P	P
Type d'événement	O	C(=)
Heure de l'événement	P	–
Informations d'événement Cause de rapport de service	C	–
Identificateur de notification	U	–
Notifications corrélées	U	–
Texte additionnel	U	–
Information additionnelle	U	–
Heure actuelle	–	P
Réponse à l'événement	–	–
Erreurs	–	P

Les paramètres heure de l'événement, notifications corrélées et identificateur de notification peuvent être assignés par l'objet géré qui émet la notification, ou par le système géré.

10 Unités fonctionnelles

La fonction de piste de vérification de sécurité constitue une seule unité fonctionnelle de gestion des systèmes.

11 Protocole

11.1 Eléments de procédure

11.1.1 Rôle d'agent

11.1.1.1 Invocation

Les procédures de rapport de piste de vérification de sécurité sont lancées par la primitive de demande de rapport de piste de vérification de sécurité. A la réception d'une telle primitive, la SMAPM doit construire une MAPDU et envoyer une primitive de service CMIS de demande G-RAPPORT-ÉVÉNEMENT avec des paramètres obtenus de la primitive de demande de rapport de piste de vérification de sécurité. En mode non confirmé, la procédure décrite en 11.1.1.2 n'est pas applicable.

11.1.1.2 Réception de la réponse

A la réception d'une primitive de service CMIS de confirmation G-RAPPORT-ÉVÉNEMENT contenant une MAPDU répondant à une notification de rapport de piste de vérification de sécurité, la SMAPM doit envoyer une primitive de confirmation de rapport de piste de vérification de sécurité à l'utilisateur du service de rapport de piste de vérification de sécurité, avec des paramètres obtenus de la primitive de service CMIS de confirmation G-RAPPORT-ÉVÉNEMENT, achevant ainsi la procédure de rapport de piste de vérification de sécurité.

REMARQUE – La SMAPM doit ignorer toutes les erreurs dans la MAPDU reçue. L'utilisateur du service de rapport de piste de vérification de sécurité peut ignorer de telles erreurs, ou peut rompre l'association suite à de telles erreurs.

11.1.2 Rôle de gestionnaire

11.1.2.1 Réception de la demande

A la réception d'une primitive de service CMIS d'indication G-RAPPORT-ÉVÉNEMENT contenant une MAPDU demandant le service rapport de piste de vérification de sécurité, et si la MAPDU est correctement construite, la SMAPM doit envoyer une primitive d'indication de rapport de piste de vérification à l'utilisateur du service rapport de piste de vérification de sécurité, avec des paramètres obtenus de la primitive de service CMIS d'indication G-RAPPORT-ÉVÉNEMENT. Autrement, la SMAPM doit, en mode confirmé, construire une MAPDU appropriée contenant la notification de l'erreur et doit envoyer une primitive de service CMIS de réponse G-RAPPORT-ÉVÉNEMENT avec un paramètre d'erreur présent. En mode non confirmé, la procédure décrite en 11.1.2.2 n'est pas applicable.

11.1.2.2 Réponse

En mode confirmé, la SMAPM doit accepter une primitive de réponse de rapport de piste de vérification de sécurité, construire une MAPDU confirmant la notification et émettre une primitive de service CMIS de réponse G-RAPPORT-ÉVÉNEMENT avec les paramètres obtenus de la primitive de réponse de rapport de piste de vérification.

11.2 Syntaxe abstraite

11.2.1 Objets gérés

La présente Recommandation | Norme internationale définit l'objet de support suivant, dont la syntaxe abstraite est spécifiée dans l'annexe A:

securityAuditTrailRecord (enregistrement de piste de vérification de sécurité)

11.2.2 Attributs

Le tableau 2 identifie la relation entre le paramètre défini en 8.1.2 et la spécification de type d'attribut donnée dans l'annexe A.

Tableau 2 – Attributs

Paramètre	Nom d'attribut
Cause de rapport de sécurité	serviceReportCause

11.2.3 Groupes d'attributs

La présente fonction de gestion de systèmes ne définit pas de groupe d'attributs.

11.2.4 Actions

La présente fonction de gestion de systèmes ne définit pas d'action spécifique.

11.2.5 Notifications

Le tableau 3 identifie la relation entre les notifications définies en 8.1.1 et les spécifications de type de notification données dans l'annexe A.

Tableau 3 – Notifications

Type de piste de vérification de sécurité	Type de notification
Rapport de service	serviceReport
Rapport d'utilisation	usageReport

La syntaxe abstraite à laquelle les spécifications de type de notification font référence est acheminée dans la MAPDU.

11.2.6 Causes de rapport de service

Le tableau 4 identifie la relation entre les causes de rapport de service définies en 8.1.2 et les références de valeur de l'ASN.1 définies dans l'annexe A.

Tableau 4 – Causes de rapport de service

Cause de rapport de service	Référence de valeur ASN.1
Demande de service	serviceRequest
Refus de service	serviceDenial
Réponse du service	serviceResponse
Défaillance du service	serviceFailure
Reprise de service	serviceRecovery
Autre raison	otherReason

11.3 Négociation des unités fonctionnelles de rapport de piste de vérification de sécurité

La présente Recommandation | Norme internationale attribue l'identificateur d'objet

{joint-iso-ccitt ms(9) function(2) part8(8) functionalUnitPackage (1)}

comme valeur pour le type FunctionalUnitPackageId de l'ASN.1, défini dans la Rec. X.701 du CCITT | ISO/CEI 10040 pour être utilisé dans les négociations de l'unité fonctionnelle suivante:

0 unité fonctionnelle de rapport de piste de vérification de sécurité

où le nombre indique la position du bit attribué à l'unité fonctionnelle conformément à l'article 10.

La Rec. X.701 du CCITT | ISO/CEI 10040 décrit le mécanisme de négociation de l'unité fonctionnelle de rapport de piste de vérification de sécurité dans le contexte d'application de gestion de systèmes.

REMARQUE – Les exigences de négociation des unités fonctionnelles sont spécifiées par le contexte d'application.

12 Relations avec d'autres fonctions

La commande du service de rapport de piste de vérification de sécurité est assurée par les mécanismes spécifiés dans la Rec. X.734 du CCITT | ISO/CEI 10164-5. La Rec. X.735 du CCITT | ISO/CEI 10164-6 assure la modification des attributs de registre de consignation de piste de vérification de sécurité.

Le service de notification de piste de vérification de sécurité peut exister indépendamment des services de commande définis dans la Rec. X.734 du CCITT | ISO/CEI 10164-5 et la Rec. X.735 du CCITT | ISO/CEI 10164-6.

13 Conformité

Il existe deux classes de conformité: la classe de conformité générale et la classe de conformité induite. Tout système prétendant mettre en œuvre des éléments de procédure pour l'unité fonctionnelle de rapport de piste de vérification de sécurité définie dans la présente Recommandation | Norme internationale doit être conforme aux spécifications de la classe de conformité générale ou induite, telles qu'elles sont définies dans les paragraphes suivants. Le fournisseur de la mise en œuvre doit indiquer la classe avec laquelle la conformité est déclarée.

REMARQUE – L'utilisation des deux termes «classe de conformité générale» et «classe de conformité induite» fait actuellement l'objet d'une étude. Toutefois, la présente Norme continue à utiliser ces termes pour être cohérente avec la Rec. X.701 du CCITT | ISO/CEI 10040 et avec d'autres Normes figurant sous le titre général *Technologie de l'information – Interconnexion de systèmes ouverts – Gestion des systèmes*. Lorsque l'examen sera terminé, il est prévu de préciser et/ou de corriger cet article relatif à la conformité ainsi que les articles correspondants dans les autres Normes.

13.1 Spécifications de la classe de conformité générale

Un système prétendant à la conformité générale avec la présente Recommandation | Norme internationale devra assurer cette fonction de gestion de systèmes pour toutes les classes d'objet géré qui importent l'information de gestion définie dans la présente Recommandation | Norme internationale.

13.1.1 Conformité statique

Le système:

- a) assurera le rôle de gestionnaire ou d'agent ou des deux, par rapport à l'unité fonctionnelle de rapport de piste de vérification de sécurité;
- b) acceptera la syntaxe de transfert dérivée des règles de codage spécifiées dans la Rec. X.209 du CCITT | ISO/CEI 8825, nommée

{joint-iso-ccitt asn1(1) basic encoding(1)}

aux fins de génération et d'interprétation des unités MAPDU définies par les types abstraits de données auxquels l'article 11.2.5 fait référence.

13.1.2 Conformité dynamique

Le système doit assurer les éléments de procédure définis dans la présente Recommandation | Norme internationale pour le service de piste de vérification de sécurité, selon le(s) rôle(s) pour lequel (lesquels) la conformité est déclarée.

13.2 Spécifications de la classe de conformité induite

13.2.1 Conformité statique

Le système acceptera l'utilisation de la syntaxe de transfert dérivée des règles de codage spécifiées dans la Rec. X.209 du CCITT | ISO/CEI 8825, nommée

{joint-iso-ccitt asn1(1) basic encoding(1)}

aux fins de génération et d'interprétation des unités MAPDU définies par les types abstraits de données auxquels l'article 11.2.5 fait référence, selon les exigences de la spécification de référence.

13.2.2 Conformité dynamique

Le système doit assurer les éléments de procédure définis dans la présente Recommandation | Norme internationale, selon les exigences de la spécification de référence.

13.3 Spécifications de la conformité de l'information de gestion

Un formulaire MCS conforme à la présente Recommandation | Norme internationale doit être textuellement identique à celui présenté dans l'annexe B, excepté pour la pagination et les en-têtes de page. Un formulaire de déclaration de conformité MOCS pour une classe d'objet d'enregistrement de piste de vérification de sécurité qui est conforme à la présente Recommandation | Norme internationale doit être textuellement identique au formulaire de déclaration MOCS spécifié dans l'annexe C, excepté pour la pagination et les en-têtes de page. Un formulaire de déclaration MIDS pour une notification de piste de vérification de sécurité qui est conforme à la présente Recommandation | Norme internationale doit être textuellement identique au formulaire de déclaration MIDS spécifié dans l'annexe D, excepté pour la pagination et les en-têtes de page. Un système conforme à la présente Recommandation | Norme internationale doit:

- décrire une mise en œuvre conforme à la présente Recommandation | Norme internationale;
- être conforme à un formulaire MCS, MOCS ou MIDS de conformité, rempli en accord avec les instructions données dans la Rec. X.724 du CCITT | ISO/CEI 10165-6;
- inclure les informations nécessaires pour définir de manière unique le fournisseur et la mise en œuvre.

Le fournisseur d'une mise en œuvre qui prétend être conforme à la présente Recommandation | Norme internationale doit remplir une copie du résumé de conformité de gestion donné dans l'annexe B, en tant que partie des spécifications de conformité, et doit fournir les informations nécessaires pour identifier le fournisseur et la mise en œuvre.

13.4 Spécifications du PICS

Un formulaire PICS conforme à la présente Recommandation | Norme internationale doit être textuellement identique à celui présenté dans l'annexe E, excepté pour la pagination et les en-têtes de page. Un PICS conforme à la présente Recommandation | Norme internationale doit:

- décrire une mise en œuvre conforme à la présente Recommandation | Norme internationale;
- être conforme à un formulaire PICS, rempli compte tenu des instructions données en E.1;
- contenir les informations nécessaires pour définir de manière unique le fournisseur et la mise en œuvre.

Le fournisseur d'une instance de protocole qui se veut conforme à la présente Recommandation | Norme internationale doit remplir un exemplaire du formulaire PICS fourni dans l'annexe E, dans le cadre des spécifications de conformité, et doit fournir les informations nécessaires pour identifier le fournisseur et l'instance.

Annexe A

Définition de l'information de gestion

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

A.1 Attribution des identificateurs d'objet

La présente Recommandation | Norme internationale attribue les identificateurs d'objet suivants:

SecurityAuditTrailDefinitions {joint-iso-ccitt ms(9) function(2) part8(8) asn1Module(2) 1}
DEFINITIONS ::= BEGIN

securityAuditTrail-Object OBJECT IDENTIFIER ::= {joint-iso-ccitt ms(9) function(2) part8(8) managedObjectClass(3)}

securityAuditTrail-Package OBJECT IDENTIFIER ::= {joint-iso-ccitt ms(9) function(2) part8(8) package(4)}

securityAuditTrail-Attribute OBJECT IDENTIFIER ::= {joint-iso-ccitt ms(9) function(2) part8(8) attribute(7)}

securityAuditTrail-Notification OBJECT IDENTIFIER ::= {joint-iso-ccitt ms(9) function(2) part8(8) notification(10)}

serviceReportCause OBJECT IDENTIFIER ::= {joint-iso-ccitt ms(9) function(2) part8(8) standardSpecificExtension(0) 1}

-- Les valeurs suivantes d'IDENTIFICATEUR D'OBJET (OBJECT IDENTIFIER) peuvent être utilisées pour le
 -- paramètre cause de rapport de service défini en A.5

serviceRequest ServiceReportCause ::= {serviceReportCause 1}

serviceDenial ServiceReportCause ::= {serviceReportCause 2}

serviceResponse ServiceReportCause ::= {serviceReportCause 3}

serviceFailure ServiceReportCause ::= {serviceReportCause 4}

serviceRecovery ServiceReportCause ::= {serviceReportCause 5}

otherReason ServiceReportCause ::= {serviceReportCause 6}

END

A.2 Définition des classes d'objet géré

La classe d'objet securityAuditTrailRecord est utilisée pour définir l'information consignée suite aux notifications ou aux rapports d'événement de piste de vérification de sécurité.

securityAuditTrailRecord MANAGED OBJECT CLASS

DERIVED FROM "CCITT Rec. X.721 | ISO/IEC 10165-2 : 1992":eventLogRecord;

CONDITIONAL PACKAGES

serviceReportCausePackage PACKAGE

BEHAVIOUR

serviceReportCausePackageBehaviour BEHAVIOUR

DEFINED AS "This package provides further qualification as to the probable cause of a service report.";

;

ATTRIBUTES serviceReportCause GET;

REGISTERED AS {securityAuditTrail-Package 1};

PRESENT IF "This package shall be present if the notification concerns a service report.";

REGISTERED AS {securityAuditTrail-Object 1};

A.3 Définitions des attributs

serviceReportCause ATTRIBUTE

WITH ATTRIBUTE SYNTAX SecurityAuditTrail-ASN1Module.ServiceReportCause;

MATCHES FOR EQUALITY;

BEHAVIOUR

serviceReportCauseBehaviour BEHAVIOUR

DEFINED AS "This attribute is used to provide the reason for the service report. The value of this attribute is an OBJECT IDENTIFIER that has been registered by a registration authority. Some of the possible values of this attribute are specified by, and registered in this Recommendation | International Standard.";

;

REGISTERED AS {securityAuditTrail-Attribute 1};

A.4 Définition des types de notification

A.4.1 Rapport de service

serviceReport NOTIFICATION

BEHAVIOUR serviceReportBehaviour;

WITH INFORMATION SYNTAX SecurityAuditTrail-ASN1Module.SecurityAuditInfo

AND ATTRIBUTE IDS

serviceReportCause serviceReportCause,
notificationIdentifier notificationIdentifier,
correlatedNotifications correlatedNotifications,
additionalText additionalText,
additionalInformation additionalInformation;

REGISTERED AS {securityAuditTrail-Notification 1};

serviceReportBehaviour BEHAVIOUR

DEFINED AS "This notification type is used to report information about a service request, denial, response, recovery or other information which is relevant to the security administrator.";

A.4.2 Rapport d'utilisation

usageReport NOTIFICATION

BEHAVIOUR usageReportBehaviour;

WITH INFORMATION SYNTAX SecurityAuditTrail-ASN1Module.SecurityAuditInfo

AND ATTRIBUTE IDS

notificationIdentifier notificationIdentifier,
correlatedNotifications correlatedNotifications,
additionalText additionalText,
additionalInformation additionalInformation;

REGISTERED AS {securityAuditTrail-Notification 2};

usageReportBehaviour BEHAVIOUR

DEFINED AS "This notification type is used to report information of a statistical nature which is relevant to the security administrator.";

A.5 Définitions de la syntaxe abstraite

SecurityAuditTrail-ASN1Module {joint-iso-ccitt ms(9) function(2) part8(8) asn1Module(2) 2}

DEFINITIONS ::= BEGIN

IMPORTS

AdditionalText, AdditionalInformation, CorrelatedNotifications, NotificationIdentifier

FROM Attribute-ASN1Module {joint-iso-ccitt ms(9) smi(3) part2(2) asn1Module(2) 1}

SecurityAuditInfo ::= SEQUENCE {
 serviceReportCause IMPLICIT ServiceReportCause OPTIONAL,
 notificationIdentifier IMPLICIT NotificationIdentifier OPTIONAL,
 correlatedNotifications [1] IMPLICIT CorrelatedNotifications OPTIONAL,
 additionalText IMPLICIT AdditionalText OPTIONAL,
 additionalInformation [2] IMPLICIT AdditionalInformation OPTIONAL }

ServiceReportCause ::= OBJECT IDENTIFIER

END

Annexe B

Formulaire MCS³⁾

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

B.1 Introduction

B.1.1 Symbols, abbreviations and terms

The following abbreviations are used throughout the proformas:

o.N	(N is an INTEGER) support of at least one of the choices is required
dmi-att	joint-iso-ccitt ms(9) smi(3) part2(2) attribute(7)
dmi-nb	joint-iso-ccitt ms(9) smi(3) part2(2) nameBinding(6)
dmi-pkg	joint-iso-ccitt ms(9) smi(3) part2(2) package(4)
satf-att	joint-iso-ccitt ms(9) function(2) part8(8) attribute(7)
satf-not	joint-iso-ccitt ms(9) function(2) part8(8) notification(10)

B.1.2 Table format

Some of the tables in Annexes C and D have been split because the information is too wide to fit on the page. Where this occurs, the index number of the first block of columns has a lower case “a” appended, and index number of the second block of columns has a lower case “b” appended. A complete table reconstructed from the constituent parts should have the following layout.

Index	Columns associated with “a”	Columns associated with “b”
-------	-----------------------------	-----------------------------

B.2 Identification of the implementation

B.2.1 Date of statement

The supplier of the implementation shall enter the date of this statement in the box below. Use the format DD-MM-YYYY.

Date of statement

B.2.2 Identification of the implementation

The supplier of the implementation shall enter information necessary to uniquely identify the implementation and the system(s) in which it may reside, in the box below.

--

³⁾ Les utilisateurs de la présente Recommandation | Norme internationale sont autorisés à reproduire le formulaire MCS de la présente annexe pour utiliser celui-ci conformément à son objet. Ils sont également autorisés à publier le formulaire une fois celui-ci complété. Les instructions pour compléter le formulaire MCS sont spécifiées dans la Rec. X.724 du CCITT | ISO/CEI 10165-6.

B.2.3 Contact

The supplier of the implementation shall provide information on whom to contact if there are any queries concerning the content of the MCS, in the box below.

--

B.3 Identification of the Recommendation | International Standard in which the management information is defined

The supplier of the implementation shall enter the title, reference number and date of the publication of the Recommendation | International Standard which specifies the management information to which conformance is claimed, in the box below.

Recommendation International Standard to which conformance is claimed

B.3.1 Technical corrigenda implemented

The supplier of the implementation shall enter the reference numbers of implemented technical corrigenda which modify the identified Recommendation | International Standard, in the box below.

--

B.3.2 Amendments implemented

The supplier of the implementation shall state the titles and reference numbers of implemented amendments to the identified Recommendation | International Standard, in the box below.

--

B.4 Management conformance summary

The supplier of the implementation shall provide information on whether the implementation claims conformance to any of the set of Recommendations | International Standards globally representing the implementation under claim. For each Recommendation | International Standard the supplier of the implementation claims conformance to, the corresponding conformance statement(s) shall be completed, or referenced, by the MCS. The supplier of the implementation shall complete the Support and Additional information columns.

Identification of the Recommendation International Standard that includes the proforma	Reference of MOCS proforma	Managed object class template label	Status	Support	Additional information
CCITT Rec. X.740 ISO/IEC 10164-8	Annex C	securityAuditTrailRecord	m		

Annexe C

Formulaire MOCS⁴⁾

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

C.1 Statement of conformance to the managed object class

Managed object class template label	Value of OBJECT IDENTIFIER for the class
securityAuditTrailRecord	{joint-iso-ccitt ms(9) function(2) part8(8) managedObjectClass(3) 1}

The supplier of the implementation shall state whether or not all mandatory features of the security audit trail record are supported, in Table C.1.

Table C.1 – Feature support

Index		Support
C.1.1	Are all mandatory features of the managed object class supported?	
C.1.2	Do instances of the managed object class support allomorphism?	

C.2 Name bindings

The supplier of the implementation shall state which name bindings in which instances of the managed object class can be subordinate are supported, in the Support and Additional information columns of Table C.2.

Table C.2 – Name binding support

Index	Name binding template label	Value of OBJECT IDENTIFIER for name binding	Superior object class template label	Status	Support
C.2.1a	logRecord-log	{dmi-nb 3}	“CCITT Rec. X.721 ISO/IEC 10165-2 : 1992”:log AND SUBCLASSES	o	

Table C.2 (concluded) – Name binding support

Index	Status		Support		Additional information
	Object creation	Object deletion	Object creation	Object deletion	
C.2.1b	x	m			

⁴⁾ Les utilisateurs de la présente Recommandation | Norme internationale sont autorisés à reproduire le formulaire MOCS de la présente annexe pour utiliser celui-ci conformément à son objet. Ils sont également autorisés à publier le formulaire une fois celui-ci complété. Les instructions pour compléter le formulaire MOCS sont spécifiées dans la Rec. X.724 du CCITT | ISO/CEI 10165-6.

C.3 Packages

The supplier of the implementation shall state whether or not the packages specified by this managed object of this class are supported, in Table C.3.

Table C.3 – Package support

Index	Package label	Value of OBJECT IDENTIFIER	Status	Support
C.3.1	eventTimePackage	{dmi-pkg 11}	o	
C.3.2	notificationIdentifierPackage	{dmi-pkg 24}	o	
C.3.3	correlatedNotificationsPackage	{dmi-pkg 23}	o	
C.3.4	additionalTextPackage	{dmi-pkg 19}	o	
C.3.5	additionalInformationPackage	{dmi-pkg 18}	o	

C.4 Attributes

The supplier of the implementation shall state whether or not the attributes specified by all of the packages instantiated in a managed object of this class are supported, in the Support and Additional information columns of Table C.4. The supplier of the implementation shall indicate support for each of the operations for each attribute supported.

Table C.4 – Attribute support

Index	Attribute template label	Value of OBJECT IDENTIFIER	Status					
			SetByCreate	Get	Replace	Add	Remove	SetToDefault
C.4.1a	objectClass	{dmi-att 65}	x	m	x	x	x	x
C.4.2a	nameBinding	{dmi-att 63}	x	m	x	x	x	x
C.4.3a	packages	{dmi-att 66}	x	c1	x	x	x	x
C.4.4a	allomorphs	{dmi-att 50}	x	c2	x	x	x	x
C.4.5a	logRecordId	{dmi-att 3}	x	m	x	x	x	x
C.4.6a	loggingTime	{dmi-att 59}	x	m	x	x	x	x
C.4.7a	managedObjectClass	{dmi-att 60}	x	m	x	x	x	x
C.4.8a	managedObjectInstance	{dmi-att 61}	x	m	x	x	x	x
C.4.9a	eventType	{dmi-att 14}	x	m	x	x	x	x
C.4.10a	eventTime	{dmi-att 13}	x	c3	x	x	x	x
C.4.11a	notificationIdentifier	{dmi-att 16}	x	c4	x	x	x	x
C.4.12a	correlatedNotifications	{dmi-att 12}	x	c5	x	x	x	x
C.4.13a	additionalText	{dmi-att 7}	x	c6	x	x	x	x
C.4.14a	additionalInformation	{dmi-att 6}	x	c7	x	x	x	x
C.4.15a	serviceReportCause	{satf-att 1}	x	m	x	x	x	x

c1: if C.3.1 or C.3.2 or C.3.3 or C.3.4 or C.3.5 then m else –

c2: if C.1.2 then m else –

c3: if C.3.1 then m else –

c4: if C.3.2 then m else –

c5: if C.3.3 then m else –

c6: if C.3.4 then m else –

c7: if C.3.5 then m else –

Table C.4 (concluded) – Attribute support

Index	Support						Additional information
	SetByCreate	Get	Replace	Add	Remove	SetToDefault	
C.4.1b							
C.4.2b							
C.4.3b							
C.4.4b							
C.4.5b							
C.4.6b							
C.4.7b							
C.4.8b							
C.4.9b							
C.4.10b							
C.4.11b							
C.4.12b							
C.4.13b							
C.4.14b							
C.4.15b							

C.5 Attribute groups

There are no attribute groups specified for this managed object class.

C.6 Actions

There are no actions specified for this managed object class.

C.7 Notifications

There are no notifications specified for this managed object class.

C.8 Parameters

There are no parameters specified for this managed object class.

Annexe D

Formulaire MIDS (notification)⁵⁾

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

The specifier of a managed object class that claims to support the notifications specified by CCITT Rec. X.740 | ISO/IEC 10164-8 shall import a copy of this annex and complete it according to the instructions specified in CCITT Rec. X.724 | ISO/IEC 10165-6.

Table D.1 – Notification support

Index	Notification template label	Value of OBJECT IDENTIFIER	Status	Support		Additional information
				Confirmed	Non-confirmed	
D.1.1a	serviceReport	{satf-not 1}				
D.1.1.1a	–	–	–	–	–	–
D.1.1.2a	–	–	–	–	–	–
D.1.1.3a	–	–	–	–	–	–
D.1.1.4a	–	–	–	–	–	–
D.1.1.5a	–	–	–	–	–	–
D.1.2a	usageReport	{satf-not 2}				
D.1.2.1a	–	–	–	–	–	–
D.1.2.2a	–	–	–	–	–	–
D.1.2.3a	–	–	–	–	–	–
D.1.2.4a	–	–	–	–	–	–
D.1.2.5a	–	–	–	–	–	–

Table D.1 (concluded) – Notification support

Index	Notification field name label	OBJECT IDENTIFIER value of attribute type associated with the field	Status	Support	Additional information
D.1.1b	–	–	–	–	–
D.1.1.1b	ServiceReportCause	{satf-att 1}	m		
D.1.1.2b	NotificationIdentifier	{dmi-att 16}	o		
D.1.1.3b	CorrelatedNotifications	{dmi-att 12}	o		
D.1.1.4b	AdditionalText	{dmi-att 7}	o		
D.1.1.5b	AdditionalInformation	{dmi-att 6}	o		
D.1.2b	–	–	–	–	–
D.1.2.2a	ServiceReportCause	{satf-att 1}	–	–	–
D.1.2.2b	NotificationIdentifier	{dmi-att 16}	o		
D.1.2.3b	CorrelatedNotifications	{dmi-att 12}	o		
D.1.2.4b	AdditionalText	{dmi-att 7}	o		
D.1.2.5b	AdditionalInformation	{dmi-att 6}	o		

⁵⁾ Les utilisateurs de la présente Recommandation | Norme internationale sont autorisés à reproduire le formulaire MIDS de la présente annexe pour utiliser celui-ci conformément à son objet. Les instructions pour compléter le formulaire MIDS sont spécifiées dans la Rec. X.724 du CCITT | ISO/CEI 10165-6.

Annexe E

Formulaire PICS⁶⁾

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

E.1 Instructions for completing the PICS proforma

E.1.1 Purpose and structure

The purpose of this PICS proforma is to provide a mechanism whereby a supplier of an implementation of CCITT Rec. X.740 | ISO/IEC 10164-8 may provide information in a standard form. The PICS proforma is subdivided into clauses for the following categories of information:

- implementation details;
- protocol details;
- overall conformance claim;
- implementation capabilities.

E.1.2 Symbols, abbreviations and terms

The PICS proforma contained in this annex is comprised of information in a tabular form in accordance with the guidelines presented in CCITT Rec. X.291 | ISO/IEC 9646-2. The following abbreviations are used:

Spt	Support
Sts	Status
TVR	Type(s), value(s) and range(s)

The following common notations, defined in CCITT Rec. X.291 | ISO/IEC 9646-2, are used for the status (Sts) column:

m	mandatory
o	optional
o.N	(N is an integer) support of at least one of the choices is required
x	prohibited
–	not applicable

The following requirements are commonly used throughout the PICS proforma:

c1	if E.5.1 then m else –
c2	if E.5.2 or E.5.3 then m else –

The following common notations, defined in CCITT Rec. X.291 | ISO/IEC 9646-2, are used for the support (Spt) column:

N	not implemented
Y	implemented
–	not applicable

Within this PICS proforma, space has been provided for the supplier of the implementation to specify types, values and ranges of all parameters supported. It is recommended that references to additional specifications are included where appropriate (for example, to list the OBJECT IDENTIFIER values and/or ranges supported), and that these additional specifications be appended to the completed PICS proforma.

E.1.3 Scoping rules

In the Status column of the tables in this Recommendation | International Standard, a mandatory element contained within an optional or conditional constructor parameter is mandatory only if the option or condition is taken.

⁶⁾ Les utilisateurs de la présente Recommandation | Norme internationale sont autorisés à reproduire le formulaire PICS de la présente annexe pour utiliser celui-ci conformément à son objet. Ils sont également autorisés à publier le formulaire une fois celui-ci complété.

E.1.4 Instructions for completing the PICS

The supplier of the implementation shall enter an explicit statement in each of the boxes provided using the notation described in E.1.2. Specific instruction is provided in the text which preceeds each table.

E.2 Identification of the implementation

E.2.1 Date of statement

The supplier of the implementation shall enter the date of this statement in the box below. Use the format DD-MM-YYYY.

Date of statement

E.2.2 Identification of the implementation

The supplier of the implementation shall enter information necessary to uniquely identify the implementation and the system(s) in which it may reside, in the box below.

E.2.3 Contact

The supplier of the implementation shall provide information on whom to contact if there are any queries concerning the content of the PICS, in the box below.

E.2.4 Relationship with the system conformance statement

The supplier of the implementation shall provide information which describes the relationship between the PICS and the system conformance statement for the system, in the box below.

E.3 Identification of the protocol

The supplier of the implementation shall enter the title, reference number and date of the publication of the Recommendation | International Standard to which conformance is claimed, in the box below.

Recommendation | International Standard to which conformance is claimed

E.3.1 Defect reports implemented

The supplier of the implementation shall enter the reference numbers of implemented defect reports which modify the specification to CCITT Rec. X.740 | ISO/IEC 10164-8, in the box below.

--

E.3.2 Amendments implemented

The supplier of the implementation shall state the titles and reference numbers of implemented amendments to CCITT Rec. X.740 | ISO/IEC 10164-8, in the box below.

--

E.4 Global statement of conformance

The supplier of the implementation shall state whether or not all mandatory capabilities are implemented for CCITT Rec. X.740 | ISO/IEC 10164-8, in Table E.1.

Table E.1 – Capabilities

Index		Support
E.1.1	Are all mandatory capabilities implemented?	

NOTE – Answering NO to this question indicates non-conformance to the protocol standard. Non-supported mandatory capabilities are listed in the PICS below, explaining why the status of the implementation is abnormal.

Capability not implemented	Reason

E.5 Capabilities**E.5.1 Systems management functional unit support**

The supplier of the implementation shall state the capability for supporting the security audit trail reporting functional unit, in Table E.2.

Table E.2 – SMFU support

Index	Functional unit name	Status	MAPDU support	CMIS support	Support
E.2.1	Security audit trail reporting functional unit	m	serviceReport usageReport	M-EVENT-REPORT	

E.5.2 Systems management functional unit negotiation support

The supplier of the implementation shall state the capability for negotiating the use of the security audit trail reporting functional unit, in Table E.3.

Table E.3 – SMFU negotiation support

Index	Negotiation capability	Status	Support
E.3.1	Does the implementation support the negotiation of the systems management functional unit?	o	

E.5.3 Management roles

The supplier of the implementation shall state the management role for which conformance is claimed, in Table E.4.

Table E.4 – Management role support

Index	Functional unit name	Status		Support	
		Manager	Agent	Manager	Agent
E.4.1	Security audit trail reporting functional unit	o.1	o.1		

E.5.4 Parameter support

The supplier of the implementation shall state support for sending the identified parameters, in Table E.5.

Table E.5 – Parameter support

Index	Parameter name	Status	Support
E.5.1	CorrelatedNotifications	o	
E.5.2	AdditionalText	o	
E.5.3	AdditionalInformation	o	

E.5.5 MAPDU support

The supplier of the implementation shall state support for the MAPDUs in the management role(s) for which conformance is claimed, in Table E.6.

Table E.6 – MAPDU support

Index	MAPDU name	Status		Support	
		Manager	Agent	Manager	Agent
E.6.1	serviceReport	o.2	o.2		
E.6.2	usageReport	o.3	o.3		

If support for the serviceReport MAPDU in the agent role is claimed, then the supplier of the implementation shall state whether or not each parameter of the MAPDU is supported in Table E.7. The supplier of the implementation shall indicate the type, value(s) and range(s) of each parameter.

Table E.7 – Service report MAPDU (sending)

Index	Parameter name	Sts	Value	Spt	TVR
E.7.1	SecurityAuditInfo	–	–	–	–
E.7.1.1	serviceReportCause	m			
E.7.1.2	notificationIdentifier	c1			
E.7.1.3	correlatedNotifications	o			
E.7.1.3.1	correlatedNotifications	m			
E.7.1.3.2	sourceObjectInst	o			
E.7.1.3.2.1	distinguishedName	o.4			
E.7.1.3.2.2	nonSpecificForm	o.4			
E.7.1.3.2.3	localDistinguishedName	o.4			
E.7.1.4	additionalText	c2			
E.7.1.5	additionalInformation	c2			
E.7.1.5.1	identifier	m			
E.7.1.5.2	significance	m			
E.7.1.5.3	information	m			

If support for the serviceReport MAPDU in the manager role is claimed, then the supplier of the implementation shall state whether or not each parameter of the MAPDU is supported in Table E.8. The supplier of the implementation shall indicate the type, value(s) and range(s) of each parameter.

Table E.8 – Service report MAPDU (receiving)

Index	Parameter name	Sts	Value	Spt	TVR
E.8.1	SecurityAuditInfo	–	–	–	–
E.8.1.1	serviceReportCause	m			
E.8.1.2	notificationIdentifier	m			
E.8.1.3	correlatedNotifications	m			
E.8.1.3.1	correlatedNotifications	m			
E.8.1.3.2	sourceObjectInst	m			
E.8.1.3.2.1	distinguishedName	m			
E.8.1.3.2.2	nonSpecificForm	m			
E.8.1.3.2.3	localDistinguishedName	m			
E.8.1.4	additionalText	m			
E.8.1.5	additionalInformation	m			
E.8.1.5.1	identifier	m			
E.8.1.5.2	significance	m			
E.8.1.5.3	information	m			

If support for the usageReport MAPDU in the agent role is claimed, then the supplier of the implementation shall state whether or not each parameter of the MAPDU is supported in Table E.9. The supplier of the implementation shall indicate the type, value(s) and range(s) of each parameter.

Table E.9 – Usage report MAPDU (sending)

Index	Parameter name	Sts	Value	Spt	TVR
E.9.1	SecurityAuditInfo	–	–	–	–
E.9.1.1	serviceReportCause	–	–	–	–
E.9.1.2	notificationIdentifier	c1			
E.9.1.3	correlatedNotifications	o			
E.9.1.3.1	correlatedNotifications	m			
E.9.1.3.2	sourceObjectInst	o			
E.9.1.3.2.1	distinguishedName	o.5			
E.9.1.3.2.2	nonSpecificForm	o.5			
E.9.1.3.2.3	localDistinguishedName	o.5			
E.9.1.4	additionalText	c2			
E.9.1.5	additionalInformation	c2			
E.9.1.5.1	identifier	m			
E.9.1.5.2	significance	m			
E.9.1.5.3	information	m			

If support for the usageReport MAPDU in the manager role is claimed, then the supplier of the implementation shall state whether or not each parameter of the MAPDU is supported in Table E.10. The supplier of the implementation shall indicate the type, value(s) and range(s) of each parameter.

Table E.10 – Usage report MAPDU (receiving)

Index	Parameter name	Sts	Value	Spt	TVR
E.10.1	SecurityAuditInfo	–	–	–	–
E.10.1.1	serviceReportCause	–	–	–	–
E.10.1.2	notificationIdentifier	m			
E.10.1.3	correlatedNotifications	m			
E.10.1.3.1	correlatedNotifications	m			
E.10.1.3.2	sourceObjectInst	m			
E.10.1.3.2.1	distinguishedName	m			
E.10.1.3.2.2	nonSpecificForm	m			
E.10.1.3.2.3	localDistinguishedName	m			
E.10.1.4	additionalText	m			
E.10.1.5	additionalInformation	m			
E.10.1.5.1	identifier	m			
E.10.1.5.2	significance	m			
E.10.1.5.3	information	m			

Annexe F

Relation avec le cadre de vérification de sécurité

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

La présente Recommandation | Norme internationale offre des services permettant de consigner les événements relatifs à la sécurité qui peuvent servir dans une vérification de sécurité. Elle ne définit pas une vérification de sécurité ni la manière d'en effectuer une. La présente Recommandation | Norme internationale ne constitue qu'un des services complémentaires pouvant être utilisés pour enregistrer les événements relatifs à la sécurité, qui présentent un intérêt potentiel pour la vérification de sécurité.

ISO/CEI 10181-7 définit les concepts et les buts d'une vérification de sécurité et fournit une description des fonctions pertinentes. Ainsi, ISO/CEI 10181-7 décrit ce qu'on peut faire avec les informations associées aux événements relatifs à la sécurité, mais ne précise pas la manière d'enregistrer ces informations.