UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

CCITT X.736

COMITÉ CONSULTATIF
INTERNATIONAL
TÉLÉGRAPHIQUE ET TÉLÉPHONIQUE

RÉSEAUX DE COMMUNICATIONS DE DONNÉES

TECHNOLOGIES DE L'INFORMATION – INTERCONNEXION DE SYSTÈMES OUVERTS – GESTION DES SYSTÈMES: FONCTION DE SIGNALISATION DES ALARMES DE SÉCURITÉ

Recommandation X.736

Genève, 1992

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 quelques 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 nº 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.736 du CCITT a été approuvé le 17 janvier 1992. Son texte est publié, sous forme identique, comme Norme internationale ISO/CEI 10164-7.

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.

SOMMAIRE

Page

NOTE D'INFORMATION

Le tableau suivant donne une liste des 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)	Management Framework
X.701 | 10040	Aperçu général de la gestion de systèmes
X.710 | 9595	Définition du service commun de transfert d'informations de gestion
X.711 | 9596-1	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 rapport d'alarme
X.734 | 10164-5	Event Management Function
X.735 | 10164-6	Log Control Function
X.736 | 10164-7	Fonction de signalisation des alarmes de sécurité
X.740 | 10164-8	Security Audit Trail Function
REMARQUE – Cette Recommandation et la Norme internationale ne sont pas identiques, par contre elles sont alignées au point de vue technique. Les titres abrégés qui figurent en anglais correspondent aux Recommandations du CCITT qui n'ont pas encore été approuvées.	

NORME INTERNATIONALE

RECOMMANDATION DU CCITT

TECHNOLOGIES DE L'INFORMATION – INTERCONNEXION DE SYSTÈMES OUVERTS – GESTION DES SYSTÈMES: FONCTION DE SIGNALISATION DES ALARMES DE SÉCURITÉ

1 Portée

La présente Recommandation | Norme internationale définit la fonction de signalisation des alarmes de sécurité. Cette fonction est une fonction de gestion des systèmes qui peut être utilisée par un processus d'application dans un environnement de gestion centralisée ou décentralisée pour échanger des informations destinées à la gestion des systèmes, telle qu'elle est définie dans la Recommandation X.700 du CCITT | ISO/CEI 7498-4. La présente Recommandation | Norme internationale intervient dans la Couche Application spécifiée dans la Recommandation X.200 | ISO 7498; elle est définie selon le modèle fourni dans la Norme ISO/CEI 9545. Le rôle des fonctions de gestion des systèmes fait l'objet de la Recommandation X.701 du CCITT | ISO/CEI 10040. Les notifications d'alarme de sécurité définies par cette fonction de gestion des systèmes fournissent des informations concernant l'état opérationnel et la qualité de service concernant la sécurité.

Les événements relatifs à la sécurité sont liés à la fourniture de la sécurité. La politique de sécurité détermine les actions à entreprendre chaque fois qu'intervient un événement qui a trait à la sécurité. La politique de sécurité peut, par exemple, spécifier qu'un rapport d'alarme de sécurité doit être émis, qu'un enregistrement de l'événement soit fait dans registre d'audit de sécurité, qu'un compteur de seuil doit être incrémenté, que l'événement ne doit pas être pris en considération ou spécifier une combinaison de ces actions. La présente Recommandation | Norme internationale ne s'intéresse qu'à la signalisation des alarmes de sécurité.

La présente Recommandation | Norme internationale:

- fixe les spécifications d'utilisateur pour la définition du service nécessaire pour supporter la fonction de signalisation des alarmes de sécurité;
- définit le service assuré par la fonction de signalisation des alarmes de sécurité;
- spécifie le protocole qui est nécessaire pour assurer le service;
- définit les relations entre les notifications de service et de gestion;
- définit les relations avec les autres fonctions de gestion des systèmes;
- spécifie les caractéristiques de conformité.

La présente Recommandation | Norme internationale:

- ne définit pas la nature d'une réalisation quelconque destinée à assurer la fonction de signalisation des alarmes de sécurité;
- ne spécifie pas les modalités d'exécution de la gestion par l'utilisateur de la fonction de signalisation des alarmes de sécurité;
- ne définit pas la nature des interactions qui se traduisent le cas échéant, par l'utilisation de la fonction de signalisation des alarmes de sécurité;
- ne spécifie pas les services nécessaires à l'établissement et à la libération normale et anormale d'une association de gestion;
- ne définit pas d'autres notifications, définies par d'autres Recommandations | Normes internationales, qui peuvent intéresser un responsable de la sécurité.

2 Références normatives

Les Recommandations du CCITT | 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 | Norme internationale est sujette 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 | Normes internationales 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 du CCITT | 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.733 du CCITT (1992) | ISO/CEI 10164-4: 1992, *Technologies de l'information – Interconnexion de systèmes ouverts – Gestion des systèmes – Fonction rapport d'alarme.*
- Recommandation X.734[1)] du CCITT | ISO/CEI 10164-5: 1992, *Information technology – Open systems Interconnection – Systems Management: Event report management function*.
- Recommandation X.735[1)] du CCITT | ISO/CEI 10164-6: 1992, *Information technology – Open Systems Interconnection – Systems Management: Log control function*.

2.2 Paires de Recommandations du CCITT | 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)*.

---

1) Actuellement à l'état de projet de Recommandation.

– Recommandation X.209 du CCITT (1988), *Spécification des règles de codage pour la notation de syntaxe abstraite numéro 1 (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*.

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

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

  ISO 7498-2: 1988, *Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Modèle de référence de base – Partie 2: Architecture de sécurité OSI*.

– Recommandation X.700[1)] du CCITT, *Management framework definition for Open Systems Interconnection for CCITT applications*.

  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*.

2.3 Références additionnelles

– ISO/CEI 9545: 1989, *Technologies de l'information – Interconnexion de systèmes ouverts – Structures de la Couche Application*.

3 Définitions

Dans le cadre de la présente Recommandation | Norme internationale, les définitions suivantes s'appliquent.

3.1 Définitions du modèle de référence de base

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

– système ouvert;

3.2 Définitions de l'architecture de sécurité

La présente Recommandation | Norme internationale utilise le terme suivant, défini dans la Recommandation X.800 du CCITT | ISO 7498-4:

a) authentification;

b) confidentialité;

c) intégrité;

---

1) Actuellement à l'état de projet de Recommandation.

d) non-répudiation;

e) politique de sécurité;

f) service de sécurité.

3.3 Définitions du cadre général de gestion

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

– objet géré.

3.4 Définitions générales utilisées en gestion des systèmes

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

a) rôle de l'agent;

b) conformité induite;

c) conformité générale;

d) rôle du gestionnaire;

e) notification;

f) unité fonctionnelle de gestion des systèmes.

3.5 Définitions de la fonction de gestion de rapport des événements

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

– discriminateur.

3.6 Définitions des conventions de service

La présente Recommandation | Norme internationale utilise les termes suivants, définis dans la Recommanda-tion X.210 du CCITT | ISO/TR 8509:

a) utilisateur de service;

b) fournisseur de service.

3.7 Définitions de tests de conformité OSI

La présente Recommandation | Norme internationale utilise le terme suivant, défini dans la Recommandation X.290 du CCITT | ISO/CEI 9646-1:

– déclaration de conformité du système.

3.8 Définitions supplémentaires

3.8.1 **alarme de sécurité:** un événement relatif à la sécurité qui a été identifié par une politique de sécurité comme une brèche potentielle dans la sécurité.

3.8.2 **événement relatif à la sécurité:** événement considéré comme concernant la sécurité.

4 Abréviations

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

CMIS Service commun d'information de gestion (*commun management information services*)

Conf Confirmation

Ind Indication

MAPDU Unité de données du protocole d'application de gestion (*management application protocol data unit*)

OSI Interconnexion de systèmes ouverts (*open systems interconnection*)

Req Demande (*request*)

Rsp Réponse (*response*)

SMAPM Machine protocole d'application de gestion de systèmes (*systems management application protocol machine*)

5 Conventions

La présente Recommandation | Norme internationale définit, à l'aide des conventions descriptives de la Recommandation X.210 du CCITT | ISO/TR 8509, les services nécessaires à la fonction de signalisation des alarmes de sécurité. A l'article 9 la définition de chaque service comprend un tableau énumérant les paramètres des primitives de ce service. Pour une primitive donnée, la présence de chaque paramètre est indiquée par l'une des valeurs suivantes:

M Paramètre obligatoire (*mandatory*).

(=) La valeur du paramètre est égale à la valeur du paramètre de la colonne de gauche.

U L'utilisation du paramètre est facultative pour l'utilisateur du service.

– Paramètre absent dans l'interaction décrite par la primitive concernée.

C Paramètre conditionnel. La ou les conditions sont définies par le texte décrivant le paramètre.

P Paramètre soumis aux contraintes imposées par la Recommandation X.710 du CCITT | ISO/CEI 9595.

REMARQUE – Les paramètres marqués «P» au tableau 2 de la présente Recommandation | Norme internationale sont mis en correspondance directe avec les paramètres correspondants de la primitive de service CMIS, sans changer la syntaxe ou la sémantique des paramètres. Les paramètres restants servent à construire une MAPDU.

6 Spécifications

Il est nécessaire que l'utilisateur de la gestion de sécurité soit alerté chaque fois qu'un événement indiquant qu'une agression ou une agression potentielle contre le système de sécurité a été décelée. Une telle agression peut être décelée par un service de sécurité, un mécanisme de sécurité ou un autre procédé.

Une notification d'alarme de sécurité peut être générée par l'un des utilisateurs en communication ou par un système ou processus intermédiaire quelconque entre ces utilisateurs. Le rapport d'alarme de sécurité doit identifier le motif du déclenchement de l'alarme de sécurité, l'origine de la détection de l'événement concernant la sécurité, les utilisateurs appropriés et la gravité perçue, le cas échéant, d'un mauvais fonctionnement, d'une agression contre la sécurité, d'une brèche dans la sécurité, selon les spécifications de la politique de sécurité.

La présente Recommandation | Norme internationale décrit l'utilisation des services et des procédés permettant de satisfaire ces spécifications.

7 Modèle

Le modèle établi pour la signalisation des alarmes de sécurité est défini dans la Recommandation X.734 du CCITT | ISO/CEI 10164-5. L'information peut être consignée conformément à la Recommandation 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 d'alarme de sécurité, ainsi que les paramètres et la sémantique applicables.

L'ensemble des notifications, paramètres et sémantique génériques définis par la présente Recommandation | Norme internationale décrit les paramètres suivants du service G-RAPPORT D'ÉVÉNEMENT défini par la Recommandation X.710 du CCITT | ISO/CEI 9595:

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

Toutes les notifications sont des entrées potentielles dans un registre de gestion des systèmes et la présente Recommandation | Norme internationale définit une classe d'objet géré dans ce but. La Recommandation X.721 du CCITT | ISO/CEI 10165-2 définit une classe d'objet d'enregistrement de registre générique à partir de laquelle sont déduites toutes les entrées, l'information supplémentaire étant spécifiée par les paramètres d'information d'événement et de réponse à l'événement.

8.1.1 Type d'événement

Ce paramètre définit le type du rapport d'alarme de sécurité. Les types d'événement ci-après sont définis dans la présente Recommandation | Norme internationale:

- violation de l'intégrité: indique que l'information peut avoir subi une modification, une insertion ou une suppression illicite;
- violation opérationnelle: indique qu'il n'a pas été possible d'obtenir le service demandé en raison de l'indisponibilité, du mauvais fonctionnement ou d'une procédure d'invocation incorrecte du service;
- violation physique: indique qu'une ressource physique a été violée, ce qui fait supposer une agression contre la sécurité;
- violation du service ou du mécanisme de sécurité: indique qu'un service ou un mécanisme de sécurité a détecté une agression contre le système de sécurité;
- violation du domaine temporel: indique qu'un événement est survenu à un instant imprévu ou interdit.

8.1.2 Information d'événement

Les paramètres suivants constituent l'information d'événement propre à la notification.

8.1.2.1 Motif de déclenchement de l'alarme de sécurité

Ce paramètre définit les conditions complémentaires concernant le motif probable de déclenchement de l'alarme de sécurité. Associée à celle du type d'événement, sa valeur permet de déterminer les paramètres qui interviennent dans le rapport des événements d'alarmes de sécurité, et les valeurs possibles de ces paramètres.

Les valeurs du motif de déclenchement des alarmes de sécurité doivent être indiquées à l'article de comportement de la définition de la classe d'objet. La présente Recommandation | Norme internationale définit, pour le contexte d'application à la gestion des systèmes défini dans la Recommandation X.701 du CCITT | ISO/CEI 10040, des motifs de déclenchement des alarmes de sécurité qui trouvent de vastes applications dans les classes d'objet géré. Ces valeurs sont spécifiées dans la Recommandation X.721 du CCITT | ISO/CEI 10165-2. La syntaxe des motifs de déclenchement d'alarme de sécurité doit être l'identificateur d'objet du type ASN.1. D'autres motifs de déclenchement des alarmes de sécurité destinées au contexte d'application de gestion des systèmes défini dans la Recommandation X.701 du CCITT | ISO/CEI 10040 peuvent être ajoutés à la présente Recommandation | Norme internationale et enregistrés au moyen des procédures d'enregistrement définies pour les valeurs d'identificateur d'objet ASN.1 de la Recommandation X.208 du CCITT | ISO/CEI 8824.

D'autres motifs de déclenchement des alarmes de sécurité, destinés au contexte d'application de gestion des systèmes défini dans la Recommandation X.701 du CCITT | ISO/CEI 10040 peuvent être définis en dehors de la présente Recommandation | Norme internationale et enregistrés au moyen des procédures d'enregistrement définies pour les valeurs d'identificateur d'objet ASN.1 dans la Recommandation X.208 du CCITT | ISO/CEI 8824.

Le tableau 1 présente les motifs de déclenchement des alarmes de sécurité associés aux types d'alarme de sécurité recensés dans la présente Recommandation | Norme internationale.

Tableau 1 – Motifs de déclenchement des alarmes de sécurité

Type d'événement	Motifs de déclenchement de l'alarme de sécurité
Violation de l'intégrité	Information dupliquée Information manquante Détection de modification d'information Information hors séquence Information inattendue
Violation opérationnelle	Refus de service Hors service Erreur de procédure Raison non spécifiée
Violation physique	Altération frauduleuse du câble Détection d'intrusion Raison non spécifiée
Violation du service ou du mécanisme de sécurité	Echec d'authentification Brèche dans la confidentialité Echec de non-répudiation Tentative d'accès non autorisée Raison non spécifiée
Violation du domaine temporel	Information tardive Mot de passe périmé Activité en dehors de l'horaire

La présente Recommandation | Norme internationale définit les motifs suivants de déclenchement des alarmes de sécurité:

- échec d'authentification: indique qu'une demande d'authentification d'un utilisateur a échoué;
- brèche dans de la confidentialité: indique que les informations ont pu être lues par un utilisateur non autorisé;
- altération frauduleuse du câble: indique qu'une violation physique d'un moyen de communication a eu lieu;
- information tardive: indique que l'information a été reçue plus tard que prévu;
- refus de service: indique qu'une demande de service recevable a été empêchée ou interdite;
- information dupliquée: indique qu'un élément d'information a été reçu plus d'une fois et peut constituer une agression par répétition;
- information manquante: indique que l'information attendue n'a pas été reçue;
- détection de modification de l'information: indication qu'une information a été modifiée, par exemple par un mécanisme de contrôle de l'intégrité des données;

- information hors séquence: indique que l'information a été reçue dans un ordre incorrect;
- détection d'intrusion: indication d'une entrée frauduleuse possible sur le site de l'équipement, ou d'une violation de l'équipement proprement dit;
- mot de passe périmé: indique qu'un mot de passe périmé a été présenté ou utilisé;
- échec de non-répudiation: indique qu'une communication a été empêchée ou arrêtée à cause de l'échec ou de l'absence d'un service de non-répudiation;
- activité en dehors de l'horaire indique l'utilisation d'une ressource à une heure inattendue;
- hors-service: indique qu'une demande de service recevable n'a pas pu être satisfaite en raison de l'indisponibilité du fournisseur de service;
- erreur de procédure: indique qu'une procédure incorrecte a été utilisée pour invoquer un service;
- tentative d'accès non autorisée: indique qu'un mécanisme de contrôle des accès a détecté une tentative illégale d'accès à une ressource;
- information inattendue: indique qu'une information inattendue a été reçue;
- raison non spécifiée: indique qu'un événement non spécifié concernant la sécurité s'est produit.

Le spécificateur de la classe d'objets gérés doit choisir le motif de déclenchement de l'alarme de sécurité le plus spécifique correspondant au cas concerné.

8.1.2.2 Gravité de l'alarme de sécurité

Ce paramètre sert à définir l'importance de l'alarme de sécurité telle qu'elle a été perçue par l'objet géré. Les niveaux de gravité ci-après sont définis:

- indéterminé: une agression contre la sécurité a été détectée. L'intégrité du système n'est pas connue;
- critique: une brèche s'est produite dans la sécurité, qui a compromis l'intégrité du système. Celui-ci ne peut plus être considéré comme fonctionnant correctement pour assurer la politique de sécurité. La gravité peut aller jusqu'à une modification de l'information de sécurité sans l'autorisation correcte, une fuite d'information vitale pour la sécurité du système (mots de passe, clefs de codage privées, etc.) ou des brèches dans la sécurité physique;
- majeur: une brèche dans la sécurité a été détectée et l'intégrité d'informations ou de mécanismes importants a été compromise;
- mineur: une brèche dans la sécurité a été détectée et l'intégrité d'informations ou de mécanismes moins importants a été compromise;
- avertissement: une agression contre la sécurité a été détectée. La sécurité du système n'est probablement pas compromise.

8.1.2.3 Détecteur d'alarme de sécurité

Ce paramètre identifie le détecteur de l'alarme de sécurité.

8.1.2.4 Utilisateur du service

Ce paramètre identifie l'utilisateur du service dont la demande de service a abouti au déclenchement de l'alarme de sécurité.

8.1.2.5 Fournisseur du service

Ce paramètre identifie le fournisseur prévu du service qui a abouti au déclenchement de l'alarme de sécurité.

8.1.3 Réponse à l'événement

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

8.2 Objet géré

Un enregistrement d'alarme de sécurité est une classe d'objet géré déduite de la classe d'objet d'enregistrement de registre d'événements définie dans la Recommandation X.721 du CCITT | Norme ISO/CEI 10165-2. La classe d'objet d'enregistrement d'alarme de sécurité représente l'information stockée dans des registres résultant de notifications d'alarmes de sécurité.

8.3 Définitions génériques importées

Les paramètres suivants sont également utilisés; ils sont définis dans la Recommandation X.733 du CCITT | ISO/CEI 10164-4:

- information additionnelle;
- texte additionnel;
- notifications corrélées;
- identificateur de notification.

8.4 Conformité

Les définitions de classe d'objet géré supportent les fonctions définies dans la présente Recommandation | Norme internationale en incorporant la spécification des notifications au moyen d'une référence aux modèles de notification définis dans la Recommandation X.721 du CCITT | ISO/CEI 10165-2. Le mécanisme de référence est défini dans la Recommandation X.722 du CCITT | ISO/CEI 10165-4.

Une définition de classe d'objet géré qui importe une ou plusieurs des notifications d'alarme définies dans la présente Recommandation | Norme internationale est nécessaire pour chaque instance d'un rapport d'alarme de sécurité, afin de choisir le type d'alarme de sécurité et le motif de déclenchement d'une telle alarme qui traduit le plus fidèlement l'événement réel qui conduit à l'objet géré émettant la notification. La définition de la classe d'objet géré est également nécessaire pour spécifier le générateur de l'alarme de sécurité, l'utilisateur du service, le fournisseur du service; elle devra aussi préciser à l'article de comportement, comment doit être spécifié le paramètre de gravité de l'alarme de sécurité.

Pour chaque notification importée, la définition de la classe d'objet géré devra spécifier à l'article de comportement les paramètres optionnels et conditionnels qui doivent être utilisés, les conditions d'utilisation et la valeur de ces paramètres. Il est permis d'indiquer que l'utilisation d'un paramètre reste facultative.

9 Définition du service

9.1 Introduction

La présente Recommandation | Norme internationale définit un service. Les notifications d'alarme de sécurité permettent de signaler les agressions contre la sécurité, les défaillances du service et du mécanisme de sécurité et d'autres événements liés à la sécurité. Les paramètres acheminent l'information relative à l'alarme de sécurité.

9.2 Service de signalisation des alarmes de sécurité

Le service de signalisation des alarmes de sécurité utilise les paramètres définis à l'article 8 de la présente Recommandation | Norme internationale, en plus des paramètres généraux G-RAPPORT D'ÉVÉNEMENT définis dans la Recommandation X.710 du CCITT | Norme ISO/CEI 9595.

Le tableau 2 donne la liste des paramètres pour le service de signalisation des alarmes de sécurité.

Tableau 2 – Paramètres de signalisation des alarmes 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	M	C(=)
Heure d'événement	P	–
Information d'événement Motif de déclenchement de l'alarme de sécurité	M	–
Gravité de l'alarme de sécurité	M	–
Détecteur de l'alarme de sécurité	M	–
Utilisateur de service	M	–
Fournisseur de service	M	–
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 signalisation des alarmes de sécurité constitue une seule unité fonctionnelle de gestion des systèmes.

11 Protocole

11.1 Eléments de procédure

11.1.1 Rôle de l'agent

11.1.1.1 Invocation

Les procédures de signalisation des alarmes de sécurité sont déclenchées par la primitive demande de signalisation des alarmes de sécurité. A la réception d'une primitive demande de signalisation des alarmes de sécurité, la SMAPM devra construire une MAPDU et émettre une primitive de service CMIS demande G-RAPPORT D'ÉVÉNEMENT avec des paramètres déduits de la primitive demande de signalisation d'alarme de sécurité. Dans le mode non confirmé, la procédure de 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 confirmation G-RAPPORT D'ÉVÉNEMENT contenant une MAPDU émise en réponse à une notification de signalisation d'alarme de sécurité, la SMAPM devra émettre une primitive de confirmation de signalisation d'alarme de sécurité pour l'utilisateur du service de signalisation d'alarme de sécurité avec des paramètres déduits de la primitive de service CMIS confirmation G-RAPPORT D'ÉVÉNEMENT, afin d'achever la procédure de signalisation d'alarme de sécurité.

REMARQUE – La SMAPM devra ignorer les erreurs dans la MAPDU reçue. L'utilisateur du service de signalisation d'alarme de sécurité peut ignorer de telles erreurs, ou abandonner prématurément l'association à cause de ces erreurs.

11.1.2 Rôle du gestionnaire

11.1.2.1 Réception de la demande

A la réception une primitive de service CMIS indication G-RAPPORT D'ÉVÉNEMENT contenant une MAPDU demandant le service de signalisation des alarmes de sécurité, la SMAPM devra, si la MAPDU est bien constituée, envoyer une primitive indication de signalisation d'alarme de sécurité à l'utilisateur du service de signalisation des alarmes de sécurité avec des paramètres déduits de la primitive de service CMIS indication G-RAPPORT D'ÉVÉNEMENT. Autrement, la SMAPM devra en mode confirmé, construire une MAPDU appropriée contenant notification de l'erreur et émettre une primitive de service CMIS réponse G-RAPPORT D'ÉVÉNEMENT contenant un paramètre d'erreur. Dans le mode non confirmé, la procédure de 11.1.2.2 n'est pas applicable.

11.1.2.2 Réponse

Dans le mode confirmé la SMAPM devra accepter une primitive réponse de signalisation des alarmes de sécurité, construire une MAPDU confirmant la notification et émettre une primitive de service CMIS réponse G-RAPPORT D'ÉVÉNEMENT avec des paramètres déduits de la primitive réponse de signalisation des alarmes de sécurité.

11.2 Syntaxe abstraite

11.2.1 Objets gérés

La présente Recommandation | Norme internationale référence l'objet-support suivant dont la syntaxe abstraite est spécifiée dans la Recommandation X.721 du CCITT | ISO/CEI 10165-2:

– securityAlarmReportRecord (Enregistrement de signalisation d'alarme de sécurité).

11.2.2 Attributs

Le tableau 3 recense les relations entre les paramètres définis en 8.1.2 de la présente Recommandation | Norme internationale et les spécifications de type d'attribut de la Recommandation X.721 du CCITT | ISO/CEI 10165-2.

Tableau 3 – Attributs

Paramètre	Nom de l'attribut
Motif de déclenchement de l'alarme de sécurité	securityAlarmCause
Gravité de l'alarme de sécurité	securityAlarmSeverity
Détecteur de l'alarme de sécurité	securityAlarmDetector
Utilisateur du service	serviceUser
Fournisseur du service	serviceProvider

11.2.3 Groupes d'attributs

Aucun groupe d'attributs n'est défini par cette fonction de gestion des systèmes.

11.2.4 Actions

Aucune action spécifique n'est définie par cette fonction de gestion des systèmes.

11.2.5 Notifications

Le tableau 4 identifie les relations entre les notifications définies en 8.1.1 de la présente Recommandation | Norme internationale et les spécifications de type de notification de la Recommandation X.721 du CCITT | ISO/CEI 10165-2.

Tableau 4 – Notifications

Type d'alarme de sécurité	Type de notification
Violation de l'intégrité	integrityViolation
Violation opérationnelle	operationalViolation
Violation physique	physicalViolation
Violation du service ou du mécanisme de sécurité	securityServiceOrMechanismViolation
Violation du domaine temporel	timeDomainViolation

La syntaxe abstraite dénotée par les spécifications de type de notification est transportée par la MAPDU.

11.2.6 Motifs de déclenchement de l'alarme de sécurité

Le tableau 5 identifie les relations entre les motifs de déclenchement de l'alarme de sécurité définis en 8.1.2.1 de la présente Recommandation | Norme internationale et les références de valeur ASN.1 définies dans la Recommandation X.721 du CCITT | ISO/CEI 10165-2.

Tableau 5 – Motifs de déclenchement des alarmes de sécurité

Motifs de déclenchement des alarmes de sécurité	Référence de valeur ASN.1
Echec d'authentification	authentificationFailure
Brèche dans la confidentialité	breachOfConfidentiality
Altération frauduleuse du câble	cableTamper
Information tardive	delayedInformation
Refus de service	denialOfService
Information dupliquée	duplicateInformation
Information manquante	informationMissing
Détection de modification de l'information	informationModificationDetected
Information hors séquence	informationOutOfSequence
Détection d'intrusion	intrusionDetection
Mot de passe périmé	keyExpired
Echec de non-répudiation	nonRepudiationFailure
Activité en dehors de l'horaire	outOfHoursActivity
Hors-service	outOfService
Erreur de procédure	proceduralError
Tentative d'accès non autorisée	unauthorizedAccessAttempt
Information inattendue	unexpectedInformation
Raison non spécifiée	unspecifiedReason

11.2.7 Valeurs de gravité des alarmes de sécurité

Le tableau 6 identifie les relations entre les valeurs définies pour le paramètre de gravité des alarmes de sécurité en 8.1.2.2 de la présente Recommandation | Norme internationale et les références de valeur ASN.1 définies dans la Recommandation X.721 du CCITT | Norme ISO/CEI 10165-2.

Tableau 6 – Valeurs de gravité des alarmes de sécurité

Gravité de l'alarme de sécurité	Référence de valeur ASN.1
Indéterminée	indeterminate
Critique	critical
Majeure	major
Mineure	minor
Avertissement	warning

11.3 Négociation de l'unité fonctionnelle de signalisation des alarmes de sécurité

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

{joint-iso-ccitt ms(9) function(2) part7(7) functionalUnitPackage(1)}

comme valeur du type ASN.1 FunctionalUnitPackageId définie dans la Recommandation X.701 du CCITT | ISO/CEI 10040, à utiliser pour négocier l'unité fonctionnelle suivante:

0 unité fonctionnelle de signalisation des alarmes de sécurité

où le nombre désigne la position de bit assignée à l'unité fonctionnelle et où le nom dénote l'unité fonctionnelle définie à l'article 10.

Dans le contexte d'application à la gestion des systèmes, le mécanisme pour négocier l'unité fonctionnelle de signalisation des alarmes de sécurité est décrit dans la Recommandation X. 701 du CCITT | ISO/CEI 10040.

REMARQUE – L'obligation de négocier des unités fonctionnelles est spécifiée par le contexte d'application.

12 Relations avec les autres fonctions

Ce sont les mécanismes spécifiés dans la Recommandation X. 734 du CCITT | ISO/CEI 10164-5 qui contrôlent le service de signalisation des alarmes de sécurité. Ce service peut exister indépendamment des mécanismes de contrôle de la Recommandation X.734 du CCITT | ISO/CEI 10164-5.

13 Conformité

Il existe deux classes de conformité: la classe de conformité générale et la classe de conformité dépendante. Un système qui prétend appliquer les éléments de procédure aux services de gestion des systèmes définis dans la présente Recommandation | Norme internationale doit satisfaire aux spécifications de la classe de conformité générale ou dépendante définies ci-dessous. Le fournisseur de l'instance doit déclarer la classe de conformité à laquelle l'instance prétend.

13.1 Spécifications de la classe de conformité générale

Un système qui prétend à une conformité générale avec la présente Recommandation | Norme internationale doit admettre cette fonction de gestion des systèmes pour toutes les classes d'objet géré qui importent une information de gestion définie dans la présente Recommandation | Norme internationale.

13.1.1 Conformité statique

Le système doit:

a) assurer le rôle du gestionnaire ou de l'agent, ou les deux, vis-à-vis de l'unité fonctionnelle de signalisation des alarmes de sécurité;

b) supporter la syntaxe de transfert déduite des règles de codage spécifiées dans la Recommandation X.209 du CCITT | ISO/CEI 8825 appelées

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

pour générer et interpréter les MAPDU, définies par les types de données abstraites dénotés en 11.2.5.

13.1.2 Conformité dynamique

Dans le ou les rôles pour lesquels une conformité est prétendue, le système doit supporter les éléments de procédure définis dans la présente Recommandation | Norme internationale pour le service de signalisation des alarmes de sécurité.

13.2 Exigences de la classe de conformité dépendante

13.2.1 Conformité statique

Le système doit:

a) fournir une déclaration de conformité du système qui identifie l'emploi normalisé de cette fonction de gestion des systèmes;

b) admettre la syntaxe de transfert déduite des règles de codage spécifiées dans la Recommandation X.209 du CCITT | ISO/CEI 8825 et appelées

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

pour générer et interpréter les MAPDU, définies par les types de données abstraites référencés en 11.2.5 comme l'exige l'emploi normalisé de cette fonction de gestion des systèmes.

13.2.2 Conformité dynamique

Le système doit admettre l'élément de procédure défini dans la présente Recommandation | Norme internationale, comme l'exige l'emploi normalisé de cette fonction de gestion des systèmes.