



UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T

X.831

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

(04/95)

**RÉSEAUX DE COMMUNICATION DE DONNÉES ET
COMMUNICATION ENTRE SYSTÈMES OUVERTS
SÉCURITÉ**

**TECHNOLOGIES DE L'INFORMATION –
INTERCONNEXION DES SYSTÈMES
OUVERTS – SÉCURITÉ GÉNÉRIQUE
DES COUCHES SUPÉRIEURES: DÉFINITION
DU SERVICE ASSURÉ PAR L'ÉLÉMENT
DE SERVICE D'ÉCHANGE DE SÉCURITÉ**

Recommandation UIT-T X.831

(Antérieurement «Recommandation du CCITT»)

AVANT-PROPOS

L'UIT (Union internationale des télécommunications) est une institution spécialisée des Nations Unies dans le domaine des télécommunications. L'UIT-T (Secteur de la normalisation des télécommunications) est un organe permanent de l'UIT. Au sein de l'UIT-T, qui est l'entité qui établit les normes mondiales (Recommandations) sur les télécommunications, participent quelque 179 pays membres, 84 exploitations de télécommunications reconnues, 145 organisations scientifiques et industrielles et 38 organisations internationales.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution n° 1 de la Conférence mondiale de normalisation des télécommunications (CMNT), (Helsinki, 1993). De plus, la CMNT, 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 de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI. Le texte de la Recommandation X.831 de l'UIT-T a été approuvé le 10 avril 1995. Son texte est publié, sous forme identique, comme Norme internationale ISO/CEI 11586-2.

NOTE

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

© UIT 1996

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.

RECOMMANDATIONS UIT-T DE LA SÉRIE X

**RÉSEAUX DE COMMUNICATION DE DONNÉES ET COMMUNICATION
ENTRE SYSTÈMES OUVERTS**

(Février 1994)

ORGANISATION DES RECOMMANDATIONS DE LA SÉRIE X

Domaine	Recommandations
RÉSEAUX PUBLICS POUR DONNÉES	
Services et services complémentaires	X.1-X.19
Interfaces	X.20-X.49
Transmission, signalisation et commutation	X.50-X.89
Aspects réseau	X.90-X.149
Maintenance	X.150-X.179
Dispositions administratives	X.180-X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	
Modèle et notation	X.200-X.209
Définition des services	X.210-X.219
Spécifications des protocoles en mode connexion	X.220-X.229
Spécifications des protocoles en mode sans connexion	X.230-X.239
Formulaires PICS	X.240-X.259
Identification des protocoles	X.260-X.269
Protocoles de sécurité	X.270-X.279
Objets gérés de couche	X.280-X.289
Test de conformité	X.290-X.299
INTERFONCTIONNEMENT DES RÉSEAUX	
Considérations générales	X.300-X.349
Systèmes mobiles de transmission de données	X.350-X.369
Gestion	X.370-X.399
SYSTÈMES DE MESSAGERIE	X.400-X.499
ANNUAIRE	X.500-X.599
RÉSEAUTAGE OSI ET ASPECTS DES SYSTÈMES	
Réseautage	X.600-X.649
Dénomination, adressage et enregistrement	X.650-X.679
Notation de syntaxe abstraite numéro un (ASN.1)	X.680-X.699
GESTION OSI	X.700-X.799
SÉCURITÉ	X.800-X.849
APPLICATIONS OSI	
Engagement, concomitance et rétablissement	X.850-X.859
Traitement des transactions	X.860-X.879
Opérations distantes	X.880-X.899
TRAITEMENT OUVERT RÉPARTI	X.900-X.999

TABLE DES MATIÈRES

	<i>Page</i>
Résumé	ii
Introduction	ii
1 Domaine d'application.....	1
2 Références normatives	1
2.1 Recommandations Normes internationales identiques.....	1
3 Définitions.....	1
4 Abréviations	2
5 Conventions.....	2
6 Aperçu général du service	2
6.1 Services spécifiques	2
6.2 Modèle de procédure du service SE-TRANSFER	2
7 Définition du service	3
7.1 Paramètres des primitives du service	3
7.2 Primitives de service	4
8 Information de mise en séquence	4

Résumé

La présente Recommandation | Norme internationale fait partie d'une série de Recommandations comprenant un ensemble de moyens destinés à la réalisation des protocoles des couches supérieures de l'OSI qui prennent en charge les services de sécurité. La présente Recommandation | Norme internationale spécifie le service fourni par l'élément de service d'échange de sécurité (SESE) qui est un élément de service d'application (ASE) facilitant la communication des informations nécessaires pour assurer les services de sécurité dans la couche Application de l'OSI.

Introduction

La présente Recommandation | Norme internationale appartient à une série de Recommandations | Normes internationales qui fournissent un ensemble de moyens destinés à la réalisation des protocoles des couches supérieures pour prendre en charge les services de sécurité. La structure de cette série est la suivante:

- Partie 1: aperçu général, modèles et notation
- Partie 2: définition du service assuré par l'élément de service d'échange de sécurité (SESE)
- Partie 3: spécification du protocole de l'élément de service d'échange de sécurité
- Partie 4: spécification de la syntaxe de protection du transfert
- Partie 5: formulaire PICS de l'élément de service d'échange de sécurité
- Partie 6: formulaire PICS de la syntaxe de protection du transfert

La présente Recommandation | Norme internationale constitue la Partie 2 de cette série.

NORME INTERNATIONALE

RECOMMANDATION UIT-T

**TECHNOLOGIES DE L'INFORMATION – INTERCONNEXION DES SYSTÈMES
OUVERTS – SÉCURITÉ GÉNÉRIQUE DES COUCHES SUPÉRIEURES:
DÉFINITION DU SERVICE ASSURÉ PAR L'ÉLÉMENT
DE SERVICE D'ÉCHANGE DE SÉCURITÉ**

1 Domaine d'application

1.1 La présente série de Recommandations | Normes internationales définit une série de moyens génériques utilisés dans l'établissement de services de sécurité dans des protocoles de couche Application. Elles comprennent:

- a) une série d'outils de notation permettant de spécifier les besoins de protection sélective des champs dans une spécification de syntaxe abstraite et permettant la spécification d'échanges de sécurité et de transformations de sécurité;
- b) une définition du service, la spécification du protocole et le formulaire PICS pour l'élément de service d'application (ASE) qui contribueront à assurer les services de sécurité dans la couche Application;
- c) une spécification et un formulaire PICS pour une syntaxe de transfert de sécurité, associés à la couche Présentation, pour les services de sécurité dans la couche Application.

1.2 La présente Recommandation | Norme internationale spécifie le service fourni par l'élément de service d'échange de sécurité (SESE). Celui-ci est un élément ASE qui permet la communication d'information de sécurité pour assurer des services de sécurité dans la couche Application.

2 Références normatives

Les Recommandations et Normes internationales suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions valables pour la présente Recommandation | Norme internationale. Au moment de la publication, les éditions indiquées étaient en vigueur. 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 Bureau de la normalisation des télécommunications de l'UIT tient à jour une liste des Recommandations de l'UIT-T en vigueur.

2.1 Recommandations | Normes internationales identiques

- Recommandation UIT-T X.200 (1994) | ISO/CEI 7498-1:1994, *Technologies de l'information – Interconnexion des systèmes ouverts – Modèle de référence de base: Le modèle de référence de base.*
- Recommandation UIT-T X.803 (1994) | ISO/CEI 10745:1995, *Technologies de l'information – Interconnexion des systèmes ouverts – Modèle de sécurité pour les couches supérieures.*

3 Définitions

Les termes suivants sont utilisés tels qu'ils sont définis dans la Rec. UIT-T X.803 | ISO/CEI 10745:

- échange de sécurité;
- item d'échange de sécurité.

4 Abréviations

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

ASE	Elément de service d'application (<i>application service element</i>)
OSI	Interconnexion des systèmes ouverts (<i>open systems interconnexion</i>)
PICS	Déclaration de conformité d'une instance de protocole (<i>protocol implementation conformance statement</i>)
SEI	Item d'échange de sécurité (<i>security exchange item</i>)

5 Conventions

L'article 7 présente sous forme de tableau les paramètres et les primitives du service SESE. Chaque paramètre est résumé au moyen de la notation suivante:

M	la présence du paramètre est obligatoire
O	la présence du paramètre est une option de la machine protocole SESE
U	la présence du paramètre est une option de l'utilisateur du service SESE
C	la présence du paramètre est conditionnelle
(=)	la valeur de ce paramètre est identique à la valeur du paramètre correspondant de la primitive de service SESE précédente

6 Aperçu général du service

L'élément de service d'échange de sécurité pourvoit à la communication d'informations associées à un échange de sécurité, comme indiqué dans la Partie 1. Ce service est généralement utilisé pour transférer des informations relatives à l'authentification, au contrôle d'accès, à la non-répudiation et à la gestion de la sécurité.

6.1 Services spécifiques

Les services suivants ont été définis:

- a) SE-TRANSFER;
- b) SE-U-ABORT;
- c) SE-P-ABORT.

Le service SE-TRANSFER est utilisé pour lancer un échange de sécurité d'un type donné, pour transférer le premier item d'échange de sécurité (SEI) et pour transférer d'autres items SEI de l'échange de sécurité. C'est le seul service requis pour réaliser un échange de sécurité.

Le service SE-U-ABORT est utilisé par l'utilisateur du service SESE pour indiquer qu'une erreur s'est produite. Ce service est utilisé pour terminer anormalement un échange de sécurité en cours. Facultativement, ce service peut également terminer anormalement une association ASO.

Le service SE-P-ABORT est utilisé par le fournisseur du service SESE pour indiquer qu'une erreur s'est produite. Il est utilisé pour terminer anormalement un échange de sécurité en cours. Facultativement, ce service peut aussi terminer anormalement une association ASO.

6.2 Modèle de procédure du service SE-TRANSFER

La Partie 1 de la présente Recommandation | Norme internationale définit le modèle de procédure suivant des échanges de sécurité:

Un item d'échange de sécurité (SEI) est transféré de A à B. Il est suivi, facultativement, d'un ou de plusieurs autres transferts d'items SEI entre A et B selon l'échange de sécurité spécifique identifié par le service SE-TRANSFER. La séquence peut se terminer à la réception de n'importe quel item SEI ou par la production d'une indication d'erreur, soit par l'utilisateur du service, soit par le fournisseur.

Le chronogramme suivant illustre le cas particulier d'une séquence de transfert d'item SEI dans les deux sens pour un échange de sécurité à n transferts. (Cet exemple relève de la classe «à l'alternat» défini au 6.1 de la Rec. UIT-T X.830 | ISO/CEI 11586-1.)



7 Définition du service

Les primitives du service SESE sont des types suivants:

SE-TRANSFER	Non confirmé
SE-U-ABORT	Non confirmé
SE-P-ABORT	Lancé par le fournisseur

7.1 Paramètres des primitives du service

Les paramètres des primitives du service sont décrits ci-après.

7.1.1 Identificateur d'échange de sécurité

Ce paramètre identifie le type particulier d'échange de sécurité dont le lancement est en cours. Quand l'échange de sécurité est défini, l'identificateur est établi au moyen de la classe d'objet d'information SECURITY-EXCHANGE définie à la Partie 1.

7.1.2 Identificateur d'invocation

Ce paramètre identifie une invocation particulière d'échange de sécurité. Il est utilisé pour se référer ultérieurement à cette invocation pour des besoins de corrélation, dans une primitive SE-TRANSFER, SE-U-ABORT ou SE-P-ABORT.

Les identificateurs d'invocation sont particulièrement utiles pour traiter des invocations d'échange de sécurité multiples dans le contexte, par exemple, d'une association d'application.

Les identificateurs d'invocation sont fournis par les utilisateurs de services qui lancent des échanges de sécurité; de tels utilisateurs sont chargés d'assurer que cet identificateur ne présente aucune ambiguïté dans le cadre de toutes les invocations d'échange de sécurité actives.

7.1.3 Item d'échange de sécurité

L'item qu'il y a lieu d'acheminer, comme cela est sous-entendu par l'identificateur d'échange de sécurité.

7.1.4 Identificateur d'item

Dans une primitive SE-TRANSFER, ce paramètre indique lequel des items de l'échange de sécurité est acheminé par cette primitive. Dans une primitive SE-U-ABORT ou SE-P-ABORT, ce paramètre indique celui des items d'un échange de sécurité sur lequel a été détectée une situation d'erreur.

La spécification d'un échange de sécurité peut imposer des contraintes spécifiques sur l'utilisation de «l'identificateur d'item». C'est l'utilisateur SESE qui est chargé de veiller à ce que ces contraintes soient respectées.

7.1.5 Fanion de début

Dans une primitive SE-TRANSFER, ce paramètre sert à indiquer le transfert du premier item d'un échange de sécurité.

7.1.6 Fanion de fin

Dans une primitive SE-TRANSFER, ce paramètre sert à indiquer que l'item d'échange de sécurité en question correspond au dernier échange de sécurité requis pour satisfaire le mécanisme de sécurité. Il est nécessaire pour prendre en charge les mécanismes nécessitant n échange, quand n n'est pas connu à l'avance.

7.1.7 Liste d'erreurs

Ce paramètre comprend une ou plusieurs listes de codes d'erreurs, comportant des paramètres d'erreur optionnels. Un code d'erreur indique la cause de l'abandon SE-U-ABORT en cours. Des codes d'erreur sont établis, lors de la définition d'un échange de sécurité, au moyen de la classe d'objets informationnels SE-ERROR, définie dans la Partie 1. Les paramètres d'erreur optionnels fournissent des informations additionnelles, décrivant la cause de l'abandon.

7.1.8 Code de problème

Ce paramètre indique la cause de l'émission de la primitive SE-P-ABORT. L'ensemble des valeurs possibles est spécifié à l'article 6 de la Partie 3.

7.1.9 Indicateur de blocage

Dans une primitive de demande SE-U-ABORT, ce paramètre est utilisé pour indiquer au fournisseur du service SESE s'il doit être mis fin à l'association ASO (par exemple, association d'application).

Dans une primitive d'indication SE-U-ABORT ou d'indication SE-P-ABORT, ce paramètre est utilisé pour indiquer à l'utilisateur du service SESE s'il doit être mis fin à l'association ASO (par exemple, association d'application).

7.2 Primitives de service

Les paramètres des primitives de service SESE sont donnés ci-dessous (voir le 6.1 qui donne la définition des services SESE et le 7.1 qui contient une description des paramètres spécifiques).

7.2.1 Service SE-TRANSFER

Les paramètres du service SE-TRANSFER se présentent comme suit:

<i>Nom du paramètre</i>	<i>Dem</i>	<i>Ind</i>
Identificateur d'échange de sécurité	M	M(=)
Identificateur d'invocation	U	C(=)
Item d'échange de sécurité	M	M(=)
Identificateur d'item	U	C(=)
Drapeau de début	U	C(=)
Drapeau de fin	U	C(=)

7.2.2 Service SE-U-ABORT

Les paramètres du service SE-U-ABORT se présentent comme suit:

<i>Nom du paramètre</i>	<i>Dem</i>	<i>Ind</i>
Identificateur d'invocation	U	C(=)
Identificateur d'item	U	C(=)
Liste d'erreurs	U	C(=)
Indicateur de blocage	U	C(=)

7.2.3 Service SE-P-ABORT

Les paramètres du service SE-P-ABORT se présentent comme suit:

<i>Nom du paramètre</i>	<i>Ind</i>
Identificateur d'invocation	O
Identificateur d'item	O
Code de problème	M
Indicateur de blocage	O

8 Information de mise en séquence

La seule contrainte de mise en séquence stipulée dans cette Définition de service est que l'invocation des primitives SE-TRANSFER ayant le même identificateur d'invocation doit être conforme aux dispositions du 7.1.2.