NORME INTERNATIONALE

ISO/CEI 10736

Première édition
1995-04-15

Technologies de l'information — Télécommunications et échange d'information entre systèmes — Protocole de sécurité de la couche transport

Information technology — Telecommunications and information exchange between systems — Transport layer security protocol

Numéro de référence
ISO/CEI 10736:1995(F)

Sommaire

ISO/CEI Copyright Office • Case postale 56 • CH-1211 Genève 20 • Suisse

Version française tirée en 1996

Imprimé en Suisse

Avant-propos

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

Dans le domaine des technologies de l'information, l'ISO et la CEI ont créé un comité technique mixte, l'ISO/CEI JTC 1. Les projets de Normes internationales adoptés par le comité technique mixte sont soumis aux organismes nationaux pour approbation, avant leur acceptation comme Normes internationales. Les Normes internationales sont approuvées conformément aux procédures qui requièrent l'approbation de 75 % au moins des organismes nationaux votants.

La Norme internationale ISO/CEI 10736 a été élaborée par le comité technique mixte ISO/CEI JTC 1, *Technologies de l'information*, sous-comité SC 6, *Téléinformatique*, en collaboration avec l'IUT-T. Le texte identique est publié en tant que Recommandation IUT-T X.274.

Les annexes A et B font partie intégrante de la présente Norme internationale. Les annexes C et D sont données uniquement à titre d'information.

Introduction

Le protocole de transport spécifié dans la Rec. UIT-T X.224 | ISO/CEI 8073 assure le service de transport en mode connexion décrit dans la Rec. UIT-T X.214 | ISO/CEI 8072. Le protocole de transport spécifié dans la Rec. UIT-T X.234 | ISO 8602 assure le service de transport en mode sans connexion décrit dans ISO 8072/AD1. La présente Recommandation | Norme internationale spécifie des fonctions optionnelles complémentaires pour les protocoles de la Rec. UIT-T X.224 | ISO/CEI 8073 et de la Rec. UIT-T X.234 | ISO 8602 permettant d'utiliser les techniques cryptographiques et d'assurer ainsi la protection des données lors de la transmission des unités de données de protocole de transport (TPDU) en mode connexion ou en mode sans connexion.

Les Annexes A et B font partie intégrante de la présente Recommandation | Norme internationale. Les Annexes C et D sont données uniquement à titre informatif.

NORME INTERNATIONALE

RECOMMANDATION UIT-T

TECHNOLOGIES DE L'INFORMATION — TÉLÉCOMMUNICATIONS ET ÉCHANGE D'INFORMATION ENTRE SYSTÈMES — PROTOCOLE DE SÉCURITÉ DE LA COUCHE TRANSPORT

1 Domaine d'application

Les procédures spécifiées dans la présente Recommandation | Norme internationale représentent des extensions des procédures définies par la Rec. UIT-T X.224 | ISO/CEI 8073 et la Rec. UIT-T X.234 | ISO 8602; elles n'interdisent en rien la communication d'informations non protégées entre des entités de transport mettant en œuvre les dispositions de la Rec. UIT-T X.224 | ISO/CEI 8073 ou de la Rec. UIT-T X.234 | ISO 8602.

La protection assurée par le protocole de sécurité défini dans la présente Recommandation | Norme internationale dépend du bon fonctionnement de la gestion de la sécurité, y compris de la gestion des clés de chiffrement. Toutefois, la présente Recommandation | Norme internationale ne spécifie pas les fonctions et protocoles de gestion nécessaires pour prendre en charge ce protocole de sécurité.

Ce protocole peut prendre en charge tous les services d'intégrité, de confidentialité, d'authentification et de contrôle d'accès identifiés dans la Rec. X.800 du CCITT / ISO 7498-2 en ce qui concerne la couche transport. Le protocole prend en charge ces services au moyen de mécanismes cryptographiques, d'étiquettes et d'attributs de sécurité, clés de chiffrement et identités authentifiées par exemple, préétablis par la gestion de la sécurité ou établis à l'aide du protocole d'association de sécurité (SA-P).

La protection ne peut être assurée que dans le cadre d'une politique de sécurité.

Ce protocole prend en charge l'authentification des entités homologues au moment de l'établissement de la connexion. En outre, la modification des clés de chiffrement est assurée, dans ce protocole, par le protocole SA-P ou par d'autres moyens qui sortent du cadre de ce protocole.

Les associations de sécurité ne peuvent être établies que dans le cadre d'une politique de sécurité. Il incombe aux utilisateurs d'établir leur propre politique de sécurité à laquelle certaines contraintes peuvent être imposées par les procédures spécifiées dans la présente Recommandation | Norme internationale.

Les éléments suivants pourraient être inclus dans une politique de sécurité:

a) méthode d'établissement/de libération de l'association SA, durée de l'association SA;

b) mécanismes d'authentification/de contrôle d'accès;

c) mécanisme d'étiquetage;

d) procédure de réception d'une TPDU non valide au cours de la procédure d'établissement d'une association SA ou de transmission d'une PDU protégée;

e) durée des clés;

f) intervalle de la procédure de modification des clés pour la mise à jour de la procédure d'échange de clés et d'informations de commande de sécurité (SCI);

g) temporisation de la procédure d'échange d'informations SCI et de modification des clés;

h) nombre de nouvelles tentatives d'échange d'informations SCI et de modification des clés.

La présente Recommandation | Norme internationale définit un protocole qui peut être mis en œuvre pour l'établissement d'une association de sécurité. Les entités qui désirent établir une association SA doivent utiliser des mécanismes communs d'authentification et de répartition de clés. La présente Recommandation | Norme internationale spécifie un algorithme, fondé sur des systèmes cryptographiques de clés publiques, pour l'authentification et la répartition de clés. La mise en œuvre de cet algorithme n'est pas obligatoire mais, lorsqu'un autre mécanisme est utilisé, il doit répondre aux conditions suivantes:

a) tous les attributs SA définis au 5.2 sont calculés;

b) les clés calculées sont authentifiées.

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 I Norme internationale. Au moment de la publication, les éditions indiquées étaient en vigueur. Toutes les Recommandations et Normes sont sujettes à révision et les parties prenantes aux accords fondés sur la présente Recommandation I Norme internationale sont invitées à étudier la possibilité d'appliquer les éditions les plus récentes des Recommandations et des Normes indiquées ci-après. Les Membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur. Le Bureau de normalisation des télécommunications de l'UIT tient à jour une liste des Recommandations de l'UIT-T actuellement en vigueur.

2.1 Recommandations I Normes internationales identiques

- Recommandation UIT-T X.214 (1993) I ISO 8072:1994, *Technologie de l'information – Interconnexion des systèmes ouverts – Définition du service de transport.*
- Recommandation UIT-T X.234 (1993) I ISO 8602:1995, *Technologie de l'information – Protocole pour assurer le service de transport en mode sans connexion.*

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

- Recommandation X.200 du CCITT (1988), *Modèle de référence de l'interconnexion des systèmes ouverts pour les applications du CCITT.*

  ISO/CEI 7498-1:1994, *Technologie de l'information – Interconnexion des systèmes ouverts – Modèle de référence de base – Partie 1: Le modèle de base.*

- 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 des systèmes ouverts – Modèle de référence de base – Partie 2: Architecture de sécurité.*

- Recommandation UIT-T X.224 (1993), *Protocole pour assurer le service de transport OSI en mode connexion.*

  ISO/CEI 8073:1992, *Technologie de l'information – Télécommunication et échange d'informations entre systèmes – Interconnexion des systèmes ouverts – Protocole pour assurer le service de transport en mode connexion.*

- Recommandation X.208 du CCITT (1988), *Spécification de la syntaxe abstraite numéro un (ASN.1).*

  ISO/CEI 8824:1990, *Technologie de l'information – Interconnexion des systèmes ouverts – Spécification de règles de base pour coder la notation de syntaxe abstraite numéro 1 (ASN.1).*

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

  ISO 8825:1990, *Technologie de l'information – Interconnexion des systèmes ouverts – Spécification des règles de base pour coder la notation de syntaxe abstraite numéro un (ASN.1).*

- Recommandation UIT-T X.264 (1993), *Mécanisme d'identification de protocole de transport.*

  ISO/CEI 11570:1992, *Technologie de l'information – Télécommunication et échange d'informations entre systèmes – Interconnexion des systèmes ouverts – Mécanisme d'identification de protocole de transport.*

2.3 Références additionnelles

- ISO/CEI 9834-1:1993, *Technologie de l'information – Interconnexion des systèmes ouverts – Procédures pour des organismes d'enregistrement particuliers – Partie 1: Procédures générales.*
- ISO/CEI 9834-3:1990, *Technologie de l'information – Interconnexion des systèmes ouverts – Procédures pour des organismes d'enregistrement particuliers – Partie 3: Enregistrement des identificateurs d'objets pour utilisation conjointement par l'ISO et le CCITT.*

3 Définitions

La présente Recommandation I Norme internationale utilise les concepts développés dans le modèle de référence pour l'interconnexion des systèmes ouverts (Rec. X.200 du CCITT I ISO 7498), y compris ceux de la Rec. X.800 du CCITT I ISO 7498-2 relatifs à l'architecture de sécurité.

3.1 Définitions reprises du modèle de référence de base

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

a) contrôle d'accès;

b) asymétrique;

c) cryptogramme;

d) texte en clair;

e) confidentialité;

f) intégrité des données;

g) authentification de l'origine des données;

h) déni de service;

i) chiffrement de bout en bout;

j) clé;

k) gestion des clés;

l) politique de sécurité;

m) symétrique.

3.2 Définitions complémentaires

Pour les besoins de la présente Recommandation I Norme internationale les définitions suivantes s'appliquent:

3.2.1 période cryptographique: Durée pendant laquelle la clé cryptographique peut être utilisée. Au-delà, la clé doit être remplacée.

3.2.2 mécanisme protocolaire dans la bande: Mécanisme protocolaire défini dans la présente Recommandation I Norme internationale.

3.2.3 mécanisme protocolaire hors bande: Mécanisme protocolaire non défini dans la présente Recommandation I Norme internationale.

3.2.4 clés jumelées: Paires de clés jumelées (clés publiques) ou identiques (clés secrètes) destinées à être utilisées entre deux correspondants donnés.

3.2.5 protection contre les réflexions: Mécanisme de protection détectant les événements de renvoi d'une unité de données de protocole vers la source.

3.2.6 association de sécurité: Relation entre deux entités en communication pour lesquelles les attributs d'association de sécurité correspondants existent.

3.2.7 attributs d'association de sécurité: Collection des informations nécessaires au contrôle de la sécurité des communications entre une entité et son ou ses homologues distantes.

3.2.8 unité de données de protocole de transport d'encapsulation de sécurité (SE TPDU): Unité de données de protocole de transport (TPDU) encapsulée pour les besoins de la sécurité et servant à expédier la TPDU définie dans la Rec. UIT-T X.224 I ISO/CEI 8073 ou dans la Rec. UIT-T X.234 I ISO 8602 après en avoir assuré la sécurité.

4 Symboles et abréviations

La présente Recommandation | Norme internationale utilise les abréviations suivantes extraites de l'article 4 de la Rec. UIT-T X.224 | ISO/CEI 8073:

TPDU CR	TPDU de demande de connexion (*connection request TPDU*)
TPDU DC	TPDU de confirmation de déconnexion (*disconnect confirm TPDU*)
TPDU DR	TPDU de demande de déconnexion (*disconnect request TPDU*)
DST-REF	[champ de] référence de l'entité destinataire (*destination reference*)
TPDU DT	TPDU de données (*data TPDU*)
TPDU ED	TPDU de données exprès (*expedited data TPDU*)
TPDU ER	TPDU d'erreur (*error TPDU*)
LI	Indicateur de longueur (*length indicator*)
NC	Connexion de réseau (*network connection*)
SN	Numéro de séquence (*sequence number*)
SRC-REF	[champ de] Référence de l'entité expéditrice (*source reference*)
TC	Connexion de transport (*transport connection*)
TPDU	Unité de données de protocole de transport (*transport protocol data unit*)

La présente Recommandation | Norme internationale utilise en outre les abréviations suivantes:

CBTSS	Service de sécurité de transport en mode connexion (*connection based transport security service*)
Conf_no	La confidentialité n'est pas à assurer
Conf_yes	La confidentialité est à assurer
DEK	Clé de codage de données (*data encipherment key*)
GTSS	Service général de sécurité de transport (*general transport security service*)
ICV	Valeur de contrôle d'intégrité (*integrity check value*)
Integ_no	L'intégrité n'est pas à assurer
Integ_yes	L'intégrité est à assurer
KEK	Clé de codage de clé (*key encipherment key*)
KEY-ID	Identificateur de clé de codage (*key identifier*)
Kg_esp	Clé cryptographique distincte pour chaque paire de systèmes terminaux (*key granularity: end system pair*)
Kg_esp_sr	Clé cryptographique distincte pour chaque paire de systèmes terminaux à chaque niveau de sécurité (*key granularity: end system pair and security level*)
Kg_tc	Clé cryptographique distincte pour chaque connexion de transport (*key granularity: transport connection*)
LABEL	Etiquette de sécurité (*security label*)
LLSG	Directives de sécurité de couches basses (*lower layer security guidelines*)
LME	Entité de gestion de couche (*layer management entity*)
MAC	Code d'authentification de message (*message authentication code*)
MDC	Code de détection de manipulation (*manipulation detection code*)
NLSP	Protocole de sécurité de la couche réseau (*network layer security protocol*)
NSAP	Point d'accès au service réseau (*network service access point*)
NSDU	Unités de données du service réseau (*network service data unit*)
PAD	[champ de] Remplissage [(*padding*) (*field*)]
Ppl_abs	Jamais d'étiquette de sécurité sur les TPDU
Ppl_pres	Etiquette de sécurité présente sur chaque TPDU

SA-P	Protocole d'association de sécurité (*security association – Protocol*)
SE TPDU	TPDU d'encapsulation de sécurité (*security encapsulation TPDU*)
TLSP	Protocole de sécurité de la couche transport (*transport layer security protocol*)

5 Vue d'ensemble du protocole

5.1 Introduction

Dans la Rec. X.800 du CCITT | ISO 7498-2, les services de sécurité suivants ont été reconnus comme relevant de la couche transport:

- authentification de l'entité homologue;
- authentification de l'origine des données;
- contrôle d'accès;
- confidentialité en mode connexion;
- confidentialité en mode sans connexion;
- intégrité en mode connexion avec reprise;
- intégrité en mode connexion sans reprise;
- intégrité en mode sans connexion.

NOTES

1 La Rec. UIT-T X.214 | ISO 8072 ne définit actuellement que 4 niveaux de qualité de protection:

a) pas de caractéristiques de protection;

b) protection contre l'écoute passive;

c) protection contre la modification, le repassage d'enregistrement, l'addition et la suppression;

d) b) et c) à la fois.

qui sont équivalentes aux services de sécurité suivants.

La Rec. X.800 du CCITT | ISO 7498-2 relative à l'architecture de sécurité OSI utilise les termes suivants pour désigner ces services de sécurité:

a) pas de services de sécurité;

b) confidentialité en mode avec ou sans connexion;

c) intégrité en mode avec ou sans connexion (avec ou sans reprise); et

d) confidentialité et intégrité à la fois en mode avec ou sans connexion.

Un rapport a été établi pour relever cette lacune dans la Rec. UIT-T X.214 | ISO 8072 et permettre la mise en place de ces sécurités et peut être aussi d'autres formes de protection.

2 L'intégrité en mode sans connexion ne protège pas contre l'addition ou la suppression des unités de données de service (SDU) et n'assure qu'une protection limitée contre le repassage d'enregistrement.

Le protocole TLSP utilisé conjointement avec le protocole de la Rec. UIT-T X.224 | ISO/CEI 8073 peut assurer l'intégrité en mode connexion avec ou sans reprise, la confidentialité en mode connexion, le service de contrôle d'accès et l'authentification de l'entité homologue, chaque connection étant protégée individuellement. Une clé peut toutefois être partagée par plusieurs connexions.

Le protocole TLSP utilisé conjointement avec le protocole de la Rec. UIT-T X.234 | ISO 8602 peut assurer l'intégrité en mode sans connexion, la confidentialité en mode sans connexion, le service de contrôle d'accès et l'authentification de l'origine des données.

La présente Recommandation | Norme internationale spécifie des extensions aux protocoles pour prendre en charge la protection de la confidentialité et de l'intégrité des données, y compris:

a) les procédures faisant intervenir des techniques cryptographiques dans le traitement protocolaire,

b) les spécifications minimales des algorithmes cryptographiques avec lesquels ces procédures peuvent être utilisées,

c) la structure et le codage des unités de données nécessaires à l'interopérabilité.

Les Figures 1 et 2 indiquent la position du protocole TLSP dans le modèle ISO à sept couches

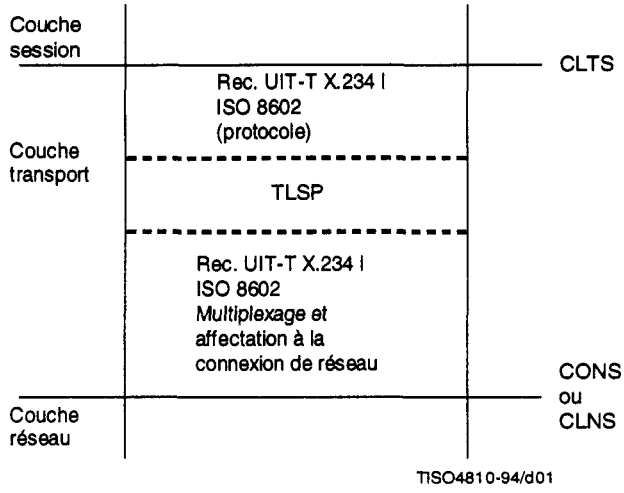

Figure 1 – Protocole TLSP dans le cadre de la Rec. UIT-T X.234 | ISO/CEI 8602

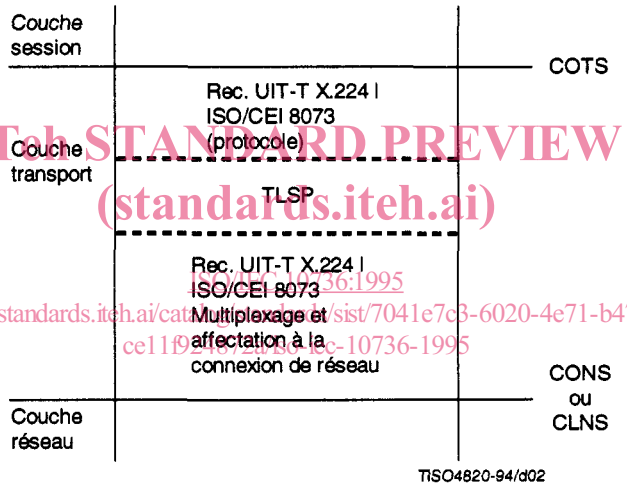

Figure 2 – Protocole TLSP dans le cadre de la Rec. UIT-T X.224 | ISO/CEI 8073

5.2 Associations et attributs de sécurité

Les options de traitement particulières du protocole TLSP utilisées dans une instance de communication sont déterminées par l'ensemble des attributs de sécurité y compris par les clés de protection jumelées. Le protocole TLSP suppose que les deux entités de transport partagent un ensemble d'attributs correspondants. L'identificateur d'association de sécurité SA-ID identifie un ensemble d'attributs qui peuvent être utilisés pour protéger une instance de communication.

Chaque association de sécurité est définie par un ensemble d'attributs caractérisant chaque système extrémal. Les moyens permettant de déterminer tous les attributs à utiliser dans une association sortent du cadre de la présente Spécification. Certains d'entre eux pourront être déterminés par un échange manuel d'attributs; d'autres pourront l'être par l'application d'un jeu agréé de règles de sécurité (ASSR) (*agreed set of security rules*). Un tel jeu est un ensemble

commun de règles spécifiant les mécanismes de sécurité à adopter, y compris tous les paramètres nécessaires pour définir le fonctionnement d'un mécanisme sélectionné pour un ou plusieurs services de protection donnés. Les règles de sécurité et leurs identificateurs peuvent être enregistrés auprès d'une tierce partie. L'Annexe C fournit un exemple illustrant un tel jeu agréé de règles de sécurité (ASSR).

D'autres attributs, tels que la durée de vie des clés et la durée limite de la procédure de redéfinition de clé, peuvent être définis dans le cadre de la politique de sécurité.

Les protocoles TLSP utilisent ces attributs d'association de sécurité pour déterminer les caractéristiques de traitement des données d'utilisateur. La suite est une description des attributs de protocole TLSP et la liste des mnémoniques utilisés pour faire référence à ces attributs dans la présente Spécification. Un ensemble d'attributs convenant à deux systèmes terminaux communiquant entre eux dépend des mécanismes utilisés et de la politique de sécurité.

a) Identificateur de l'association de sécurité (SA-ID)

1) Local_SAID: Chaîne d'octets – Identificateur local de l'association de sécurité.

2) Peer_SAID: Chaîne d'octets – Identificateur homologue distant de l'association de sécurité.

3) SAID_Len: Entier, valeur sur [2 à 126] – Longueur de l'identificateur de l'association de sécurité défini par le jeu de règles ASSR.

La valeur des attributs Local_SAID et Peer_SAID est définie au moment de l'établissement de l'association de sécurité. La valeur de SAID_Len est définie pour un jeu de règles ASSR donné.

Lorsqu'une entité de protocole TLSP détecte l'interruption d'une association de sécurité donnée, elle gèlera l'identificateur SA-ID qu'elle lui avait alloué. Tant qu'il est gelé, un identificateur ne peut pas être réutilisé. La période pendant laquelle cet identificateur restera gelé sera plus longue que la durée de vie des unités de données de protocole (PDU) du réseau sous-jacent.

b) Indicateur désignant l'entité de protocole TLSP qui joue le rôle «d'appelant» et celle qui joue le rôle «d'appelé». Cet attribut indique comment orienter l'indicateur de direction pour détecter les TPDU réfléchies.

Initiator: (appelant) – Booléen.

La valeur de cet attribut est définie au moment de l'établissement de l'association de sécurité.

c) Adresse de l'entité ou des entités de protocole TLSP homologues

Peer_adr: (adresse d'homologue) – Chaîne d'octets

La valeur de cet attribut est définie au moment de l'établissement de l'association de sécurité et indique soit l'adresse du point d'accès du service réseau (NSAP) de l'entité de transport lorsque plusieurs connexions partagent la même clé, soit l'identificateur de connexion sous la forme de numéros de référence de transport local et distant lorsque la clé correspond à une seule connexion.

d) Identificateur du jeu agréé de règles de sécurité (ASSR) adopté pour l'association en question

ASSR_ID: Identificateur d'objet tel qu'il est défini dans la syntaxe ASN.1 dans la Rec. X.208 du CCITT | ISO/CEI 8824

La valeur de cet attribut est définie au moment de l'établissement ou du pré-établissement de l'association de sécurité.

e) Qualité de service choisie pour l'association de sécurité

QOS_Label: (étiquette de QS) – Format défini par le jeu de règles ASSR

AC: (Niveau de contrôle d'accès) – Entier dont le domaine de valeurs possibles est défini par le jeu de règles ASSR

Les paramètres de qualité de service suivants n'ont de sens que pour les protocoles TLSP utilisés en conjonction avec la Rec. UIT-T X.234 | ISO 8602:

- DOAuth: (*data origin authentication level*) (niveau d'authentification de l'origine des données) Entier dont le domaine de valeurs est défini par le jeu de règles ASSR.
- CLConf: (*connectionless confidentiality level*) (niveau de confidentialité en mode sans connexion) Entier dont le domaine de valeurs est défini par le jeu de règles ASSR.
- CLInt: (*connectionless integrity level*) (niveau d'intégrité en mode sans connexion) Entier dont le domaine de valeurs est défini par le jeu de règles ASSR.