



UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T

X.274

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

(07/94)

**RÉSEAUX DE COMMUNICATION DE DONNÉES ET
COMMUNICATION ENTRE SYSTÈMES OUVERTS
INTERCONNEXION DES SYSTÈMES OUVERTS –
PROTOCOLES DE SÉCURITÉ**

**TECHNOLOGIES DE L'INFORMATION –
TÉLÉCOMMUNICATION ET ÉCHANGE
D'INFORMATIONS ENTRE SYSTÈMES –
PROTOCOLE DE SÉCURITÉ
DE LA COUCHE TRANSPORT**

Recommandation UIT-T X.274

(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 Rec. X.274 de l'UIT-T a été approuvé le 1^{er} juillet 1994. Son texte est publié, sous forme identique, comme Norme internationale ISO/CEI 10736-4.

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 1995

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 POUR DONNÉES ET INTERCONNEXION
DES 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
Système 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		iv
Introduction		v
1	Domaine d'application.....	1
2	Références normatives	2
2.1	Recommandations Normes internationales identiques.....	2
2.2	Paires de Recommandations Normes internationales équivalentes par leur contenu technique	2
2.3	Références additionnelles	2
3	Définitions.....	3
3.1	Définitions reprises du modèle de référence de base.....	3
3.2	Définitions complémentaires	3
4	Symboles et abréviations.....	4
5	Vue d'ensemble du protocole	5
5.1	Introduction	5
5.2	Associations et attributs de sécurité.....	6
5.2.1	Services de sécurité pour le protocole de transport en mode connexion	9
5.2.2	Services de sécurité pour le protocole de transport en mode sans connexion.....	10
5.3	Services assurés par la couche réseau	10
5.4	Spécifications de gestion de sécurité	10
5.5	Spécifications minimales des algorithmes	10
5.6	Fonction d'encapsulation de sécurité	10
5.6.1	Fonction de codage des données	11
5.6.2	Fonction d'intégrité	11
5.6.3	Fonction d'étiquetage de sécurité	11
5.6.4	Fonction de remplissage de sécurité	11
5.6.5	Fonction d'authentification d'entité homologue	11
5.6.6	Fonction SA utilisant le protocole SA-P dans la bande	12
6	Eléments de procédure	12
6.1	Concaténation et séparation	13
6.2	Confidentialité	13
6.2.1	Objet.....	13
6.2.2	TPDU et paramètres utilisés.....	13
6.2.3	Procédure	13
6.3	Procédure d'intégrité	14
6.3.1	Traitement de la valeur de contrôle d'intégrité (ICV)	14
6.3.1.1	Objet.....	14
6.3.1.2	TPDU et paramètres utilisés.....	14
6.3.1.3	Procédure	14
6.3.2	Traitement de l'indicateur de direction.....	16
6.3.2.1	Objet.....	16
6.3.2.2	TPDU et paramètres utilisés.....	16
6.3.2.3	Procédure	16
6.3.3	Traitement du numéro de séquence d'intégrité de connexion	17
6.3.3.1	Numéros de séquence uniques	17
6.3.3.2	Objet.....	17
6.3.3.3	Procédure	17
6.4	Traitement de la vérification d'adresse d'homologue.....	17
6.4.1	Objet.....	17
6.4.2	Procédure	17

6.5	Etiquettes de sécurité des associations de sécurité.....	18
6.5.1	Objet.....	18
6.5.2	TPDU et paramètres utilisés.....	18
6.5.3	Procédure	18
6.6	Libération de la connexion	18
6.7	Remplacement de clé	18
6.8	TPDU non protégées.....	19
6.9	Identification du protocole.....	19
6.10	Protocole d'association de sécurité	19
7	Utilisation des éléments de procédure.....	20
8	Structure et codage des TPDU	20
8.1	Structure de la TPDU.....	20
8.2	Unité d'encapsulation de sécurité TPDU	20
8.2.1	En-tête en clair	21
8.2.1.1	Longueur de l'en-tête en clair de la PDU	21
8.2.1.2	Type de PDU.....	21
8.2.1.3	Identificateur SA-ID	21
8.2.2	Synchronisation cryptographique	21
8.2.3	Contenu protégé	21
8.2.3.1	Structure des champs du contenu protégé.....	22
8.2.3.2	Champ de longueur du contenu	22
8.2.3.3	Champ Flags (fanions).....	22
8.2.3.4	Champ Label (étiquette).....	23
8.2.3.5	Champ des données protégées	23
8.2.3.6	Remplissage d'intégrité	23
8.2.4	ICV.....	24
8.2.5	Remplissage de codage	24
8.3	PDU d'association de sécurité.....	24
8.3.1	LI.....	24
8.3.2	Type de PDU.....	24
8.3.3	SA-ID.....	24
8.3.4	Type de SA-P.....	24
8.3.5	Contenu de SA PDU	25
9	Conformité	25
9.1	Considérations générales	25
9.2	Spécifications communes de conformité statique.....	25
9.3	Spécifications de conformité statique du protocole TLSP avec le protocole de la Rec. UIT-T X.234 ISO 8602.....	25
9.4	Spécifications de conformité statique du protocole TLSP avec le protocole de la Rec. UIT-T X.224 ISO/CEI 8073	25
9.5	Spécifications communes de conformité dynamique.....	25
9.6	Spécifications de conformité dynamique du protocole TLSP avec le protocole de la Rec. UIT-T X.234 ISO 8602.....	25
9.7	Spécifications de conformité dynamique du protocole TLSP avec le protocole de la Rec. UIT-T X.224 ISO/CEI 8073	26
10	Déclaration de conformité d'une instance de protocole (PICS).....	26
Annexe A	– Formulaire PICS	27
A.1	Introduction	27
A.1.1	Background.....	27
A.1.2	Approach.....	27
A.2	Implementation identification.....	28
A.3	General statement of conformance	28
A.4	Protocol implementation.....	28
A.5	Security services supported	28
A.6	Supported functions	30
A.7	Supported Protocol Data Units (PDUs).....	33

	<i>Page</i>
A.7.1	Supported Transport PDUs (TPDUs) 33
A.7.2	Supported parameters of issued TPDUs 33
A.7.3	Supported parameters of received TPDUs 33
A.7.4	Allowed values of issued TPDU parameters 34
A.8	Service, function, and protocol relationships 35
A.8.1	Relationship between services and functions 35
A.8.2	Relationship between services and protocol 35
A.9	Supported algorithms 36
A.10	Error handling 36
A.10.1	Security errors 36
A.10.2	Protocol errors 36
A.11	Security Association 36
A.11.1	SA Generic Fields 36
A.11.2	Content Fields Specific to Key Exchange SA-P 38
Annexe B	– Protocole d'association de sécurité utilisant des mécanismes d'échange de jetons de clé et de signatures numériques 39
B.1	Vue d'ensemble 39
B.2	Echange de jetons de clé (KTE) 40
B.3	Authentification de protocole SA 40
B.4	Négociation d'attributs SA 41
B.4.1	Négociation des services 41
B.4.2	Négociation de l'ensemble d'étiquettes 41
B.4.3	Sélection de clés et de numéros ISN 41
B.4.4	Négociation de divers attributs SA 42
B.4.5	Vue d'ensemble de la modification de clés 42
B.4.6	Vue d'ensemble de la procédure d'abandon/de libération d'une association SA 42
B.5	Mise en correspondance des fonctions de protocole SA avec les échanges de données de protocole 43
B.5.1	(Premier) Echange de jetons de clé (KTE) 43
B.5.1.1	Demande d'initialisation d'un protocole SA 43
B.5.1.2	Réception de la PDU du premier échange par l'entité destinataire 43
B.5.2	(Deuxième) Echange de négociation de l'authentification et de la sécurité 44
B.5.2.1	Réception de la PDU du premier échange par l'entité initiatrice 44
B.5.2.2	Réception de la PDU du deuxième échange par l'entité destinataire 44
B.5.3	Procédure de modification de clés 45
B.5.4	Echange pour la libération/l'abandon de l'association SA 46
B.5.4.1	Demande d'initialisation de la libération/de l'abandon de l'association SA ... 46
B.5.4.2	Réception d'une demande d'abandon/de libération SA 46
B.6	SA PDU – Contenu SA 47
B.6.1	ID d'échange 47
B.6.2	Longueur de contenu 47
B.6.3	Champs de contenu 47
B.6.3.1	My_SA-ID 48
B.6.3.2	Old Your-SA-ID 48
B.6.3.3	Key Token 1 et Key Token 2, Key Token 3 et Key Token 4 48
B.6.3.4	Signature numérique d'authentification, Certificat 48
B.6.3.5	Sélection de services 48
B.6.3.6	Raison du rejet SA 48
B.6.3.7	Raison de l'abandon/la libération SA 49
B.6.3.8	Label 49
B.6.3.9	Sélection de clés 49
B.6.3.10	Marqueurs SA 50
B.6.3.11	ASSR 50
Annexe C	– Exemple d'ensemble agréé de règles de sécurité (ASSR) 51
Annexe D	– Vue d'ensemble de l'algorithme EKE 52

Résumé

La présente Recommandation | Norme internationale spécifie le protocole pouvant prendre en charge les services d'intégrité, de confidentialité, d'authentification et de contrôle d'accès identifiés dans le modèle de sécurité OSI comme relevant de la couche transport. Le protocole prend en charge ces services au moyen de mécanismes cryptographiques, d'étiquetages de sécurité et d'attributs (clés de chiffrement par exemple) préétablis par la gestion de sécurité.

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 –
TÉLÉCOMMUNICATION ET ÉCHANGE D'INFORMATIONS 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 | 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 | 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 | Normes internationales identiques

- Recommandation UIT-T X.214 (1993) | ISO 8072:1994, *Technologie de l'information – Interconnexion des systèmes ouverts – Définition du service de transport.*
- Recommandation UIT-T X.234 (1993) | ISO 8602:1987, *Technologie de l'information – Interconnexion des systèmes ouverts – Protocole pour assurer le service de transport en mode sans connexion.*

2.2 Paires de Recommandations | 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 7498:1984, *Systèmes de traitement de l'information – Interconnexion des systèmes ouverts – Modèle de référence 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 7498/AD1:1987, *Systèmes de traitement de l'information – Interconnexion des systèmes ouverts – Modèle de référence de base Additif I – Transmission en mode sans connexion.*
- ISO 8072/AD1:1986, *Systèmes de traitement de l'information – Interconnexion des systèmes ouverts – Définition du service de transport Additif 1 – Transmission en mode sans connexion.*
- 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 | Norme internationale utilise les concepts développés dans le modèle de référence pour l'interconnexion des systèmes ouverts (Rec. X.200 du CCITT | ISO 7498), y compris ceux de la Rec. X.800 du CCITT | ISO 7498-2 relatifs à l'architecture de sécurité.

3.1 Définitions reprises du modèle de référence de base

La présente Recommandation | Norme internationale utilise les termes suivants définis dans la Rec. X.800 du CCITT | 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 | 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 | Norme internationale.

3.2.3 mécanisme protocolaire hors bande: Mécanisme protocolaire non défini dans la présente Recommandation | 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 | ISO/CEI 8073 ou dans la Rec. UIT-T X.234 | 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 (<i>connection request TPDU</i>)
TPDU DC	TPDU de confirmation de déconnexion (<i>disconnect confirm TPDU</i>)
TPDU DR	TPDU de demande de déconnexion (<i>disconnect request TPDU</i>)
DST-REF	[champ de] référence de l'entité destinataire (<i>destination reference</i>)
TPDU DT	TPDU de données (<i>data TPDU</i>)
TPDU ED	TPDU de données exprès (<i>expedited data TPDU</i>)
TPDU ER	TPDU d'erreur (<i>error TPDU</i>)
LI	Indicateur de longueur (<i>length indicator</i>)
NC	Connexion de réseau (<i>network connection</i>)
SN	Numéro de séquence (<i>sequence number</i>)
SRC-REF	[champ de] Référence de l'entité expéditrice (<i>source reference</i>)
TC	Connexion de transport (<i>transport connection</i>)
TPDU	Unité de données de protocole de transport (<i>transport protocol data unit</i>)

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

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

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

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 connexion 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

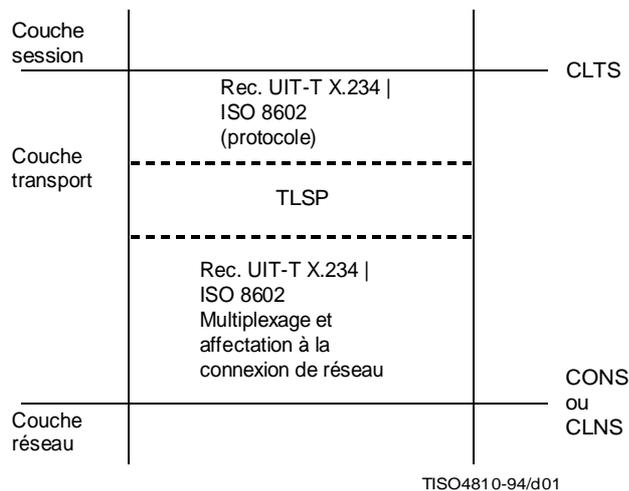


Figure 1 – Protocole TLSP dans le cadre de la Rec. UIT-T X.234 | ISO/CEI 8602

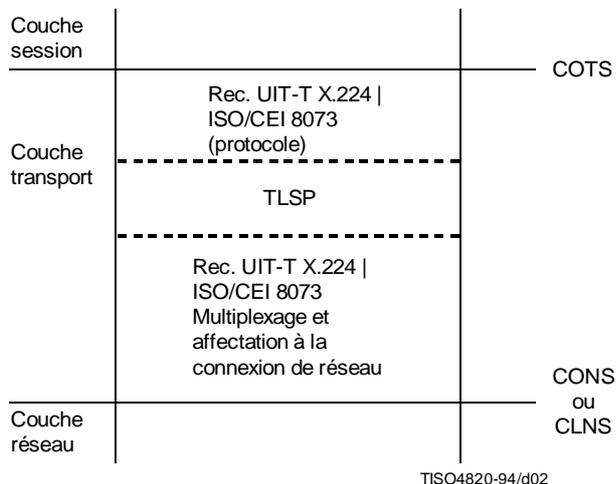


Figure 2 – Protocole TLSP dans le cadre de la Rec. UIT-T X.224 | ISO/CEI 8073

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.

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.224 | ISO 8073:

- Auth: (*peer entity authentication level*) (niveau d'authentification de l'entité homologue) Entier dont le domaine de valeurs est défini par le jeu de règles ASSR.
- COConf: (*connection confidentiality level*) (niveau de confidentialité en mode connexion) Entier dont le domaine de valeurs est défini par le jeu de règles ASSR.
- COInt: (*connection integrity without recovery*) (niveau d'intégrité en mode connexion sans reprise) Entier dont le domaine de valeurs est défini par le jeu de règles ASSR.
- COIntr: (*connection integrity with recovery*) (niveau d'intégrité en mode connexion avec reprise) 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.

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

f) Mécanismes sélectionnés pour l'association de sécurité

- Label: Booléen – Etiquetage explicite des TPDU.
- Conf: Booléen – Confidentialité d'un transfert de données sûr par codage.
- ICV: (*integrity check value*) (valeur de contrôle d'intégrité) – Booléen – Intégrité d'un transfert de données sûr par utilisation d'une valeur de contrôle d'intégrité.
- SN: (*sequence number*) (numéro de séquence) – Booléen – Intégrité de connexion par procédure de numéro de séquence.
- PE-Authentication (*peer entity authentication*) (authentification de l'entité homologue) – Booléen – Authentification de l'entité homologue par l'échange d'unités de données de protocole PDU encapsulées de demande de connexion et de réponse de connexion.
- UNProt: (non protégé) – Booléen – TPDU non protégées.

g) Attributs du mécanisme d'étiquetage

Les valeurs de ces attributs sont définies préalablement ou lors de l'établissement de l'association de sécurité. Ces attributs spécifient l'ensemble des étiquettes de sécurité qu'il est possible d'allouer à l'association de sécurité.

Label_set: Set of {

Label_Ref: (réf d'étiqu.) Entier
 Label_Defining_Auth: (aut. de déf. d'étiqu.) Identificateur d'objet
 Label_Content: (contenu d'étiqu.) Format défini par Label_Defining_Auth
 }

h) Attributs du mécanisme ICV (valeur de contrôle d'intégrité)

- ICV_Alg: (algorithme ICV) – Identificateur d'objet
- ICV_Len: (longueur ICV) – Entier
- ICV_Blck: Entier – dimension de block de remplissage pour l'algorithme ICV.

Les attributs suivants ne sont présents que si l'algorithme est du type cryptographique.

- ICV_Kg: (granularité de clé ICV) – Entier de valeur Kg_tc ou Kg_esp ou Kg_esp_sr

La clé peut avoir une des granularités suivantes:

- Kg_tc: Une clé cryptographique distincte est utilisée pour chaque connexion de transport
- Kg_esp: Une clé cryptographique distincte est utilisée pour chaque couple de systèmes terminaux
- Kg_esp_sr: Une clé cryptographique distincte est utilisée pour chaque couple de systèmes terminaux et pour chaque niveau de sécurité.

Les valeurs des attributs ci-dessus sont définies par le jeu de règles ASSR pour une qualité de service de protection donnée.

- ICV_Gen_Key: (*ICV generation key reference*) (référence de clé de génération ICV) – Forme définie par le jeu de règles ASSR
- ICV_Check_Key: (*ICV check key reference*) (référence de clé de contrôle ICV) – Forme définie par le jeu de règles ASSR

i) Attributs du mécanisme de numéro de séquence SN

Les attributs suivants n'ont de sens que pour un protocole TLSP utilisé en conjonction avec le protocole de la Rec. UIT-T X.224 | ISO/CEI 8073.

- Data_Local_SN: (SN local de données) Numéro de séquence des dernières données normales envoyées
- Data_Peer_SN: (SN homologue de données) Numéro de séquence des dernières données normales reçues

Les valeurs initiales de ces attributs sont définies dans le cadre de l'établissement normal de la connexion. SN est le numéro de séquence utilisé par le protocole de la Rec. UIT-T X.224 | ISO/CEI 8073.

j) Attributs du mécanisme de numéro de séquence de données exprès EXSN

Les attributs suivants n'ont de sens que pour un protocole TLSP utilisé en conjonction avec la Rec. UIT-T X.224 | ISO/CEI 8073.

- Data_Local_EXSN: (EXSN local de données) Numéro de séquence des dernières données exprès normales envoyées
- Data_Peer_EXSN: (EXSN homologue de données) Numéro de séquence des dernières données exprès normales reçues

Les valeurs initiales de ces attributs sont définies dans le cadre de l'établissement normal de la connexion. EXSN est le numéro de séquence utilisé par le protocole de la Rec. UIT-T X.224 | ISO/CEI 8073.

k) Attributs du mécanisme de codage

- Enc_Alg: (algorithme de codage) – Identificateur d'objet alloué au titre de ISO 9979
- Enc_Blkc: (bloc de codage) – Entier – Dimension du bloc de remplissage pour l'algorithme de codage
- Enc_Kgc: (granularité de clé de codage) – Entier dont la valeur est Kg_tc ou Kg_esp ou Kg_esp_sr

Les attributs de granularité de clé sont définis à l'alinéa h) ci-dessus.

La valeur de cet attribut est définie par le jeu de règles ASSR pour une qualité de service de protection donnée.

- Enc_Key: Référence de clé de codage – Forme définie par le jeu de règles ASSR
- Dec_Key: Référence de clé de décodage – Forme définie par le jeu de règles ASSR

NOTE – Des mécanismes et attributs complémentaires ainsi que des mécanismes à utilisation privée pourront être identifiés dans les futures versions de la présente Recommandation | Norme internationale.

5.2.1 Services de sécurité pour le protocole de transport en mode connexion

Lorsqu'un protocole de sécurité TLSP est utilisé pour assurer des services de sécurité en mode orienté connexion, l'entité de transport associera un identificateur d'association de sécurité SA-ID à chaque connexion de transport protégée (Kg_tc), à chaque couple de systèmes terminaux de transport (Kg_esp) ou à chaque ensemble formé par le couple de systèmes terminaux de transport muni de son niveau de sécurité (Kg_esp_sr). L'identificateur SA-ID sera créé explicitement pour la ou les connexions de transport protégées. Les services de sécurité à assurer sur la connexion sont ceux définis par l'association de sécurité. Toutes les TPDU envoyées ou reçues sur des connexions de transport protégées recevront la protection correspondant aux services définis pour l'association de sécurité. Si la granularité de clé a la valeur Kg_tc, il y aura une correspondance biunivoque entre les connexions de transport et les associations de sécurité.

Dans le cas de l'intégrité en mode connexion, les services de sécurité associés à l'association de sécurité inclueront le traitement de la valeur de contrôle d'intégrité (ICV = vrai). Toute TPDU incorrectement protégée sera éliminée à la réception. La réception de telles TPDU non protégées est un événement qui relève de la sécurité; la suite à donner à un tel événement (établir un rapport de vérification par exemple) sort toutefois du cadre de la présente Recommandation | Norme internationale.

5.2.2 Services de sécurité pour le protocole de transport en mode sans connexion

Lorsqu'un protocole de sécurité TLSP est utilisé pour fournir des services de sécurité au service de transport en mode sans connexion, l'entité de transport associera un identificateur d'association de sécurité SA-ID:

- soit à chaque couple d'entités de transport (Kg_esp);
- soit à chaque ensemble formé par le couple d'entités de transport muni de son niveau de sécurité (Kg_esp_sr).

L'entité de transport expéditrice protégera chaque TPDU conformément aux attributs associés à l'identificateur d'association de sécurité SA-ID et inscrira l'identificateur homologue (SA-ID) dans le paramètre SA-ID de l'unité d'encapsulation de sécurité SE TPDU. A la réception d'une SE TPDU, la clé spécifiée par le paramètre SA-ID sera utilisée pour décoder la TPDU et pour en vérifier la valeur de contrôle d'intégrité ICV. Toute TPDU incorrectement protégée sera éliminée à la réception. La réception de telles TPDU non protégées est un événement qui relève de la sécurité; la suite à donner à un tel événement (établir un rapport de vérification par exemple) sort toutefois du cadre de la présente Recommandation | Norme internationale.

5.3 Services assurés par la couche réseau

Les services de sécurité assurés par le protocole de sécurité de la couche transport TLSP sont indépendants de tout service de sécurité pouvant être assuré par la couche réseau.

5.4 Spécifications de gestion de sécurité

Ce protocole de sécurité nécessite que les attributs de l'association de sécurité aient été définis avant l'apparition de toute instance de communication protégée de données d'utilisateur. Ces attributs peuvent être définis au moyen de fonctions de gestion de sécurité qui sortent du cadre de la présente Recommandation | Norme internationale ou à l'aide du protocole SA-P.

Le degré de protection assuré dépend de la bonne gestion de la sécurité, y compris la gestion des clés. Les procédures de la présente Recommandation | Norme internationale supposent:

- a) qu'il existe un moyen de stockage des clés cryptographiques;
- b) que les entités de transport émettrice et réceptrice disposent toutes deux de la même clé cryptographique en cas de chiffrement symétrique; en cas de chiffrement asymétrique, les entités de transport émettrice et réceptrice n'ont pas accès aux mêmes clés cryptographiques. La présente Recommandation | Norme internationale prévoit l'utilisation du chiffrement soit symétrique soit asymétrique;
- c) les clés de chiffrement cryptographiques sont jumelées; voir 3.2.4.

La présente Recommandation | Norme internationale ne définit pas la manière de créer, de mettre à jour ou de gérer d'une façon ou d'une autre les clés cryptographiques.

5.5 Spécifications minimales des algorithmes

Les entités de transport émettrice et réceptrice doivent utiliser toutes deux le même ou les mêmes algorithmes de chiffrement. Les hypothèses relatives à ces algorithmes sont les suivantes:

- 1) Les services de confidentialité et d'intégrité seront assurés par le même algorithme ou par des algorithmes distincts.
- 2) Le codage et le décodage s'effectuent par multiples d'octets.
- 3) L'initialisation et la synchronisation cryptographique sont assurées individuellement au niveau de chaque TPDU.

La spécification d'un algorithme particulier et l'évaluation des points forts ou faibles d'algorithmes donnés sort du cadre de la présente Recommandation | Norme internationale.

5.6 Fonction d'encapsulation de sécurité

L'encapsulation est utilisée en conjonction avec la fonction de codage ou de contrôle d'intégrité afin d'assurer les services de confidentialité et d'intégrité en mode avec ou sans connexion. La fonction de codage a toujours un but cryptographique alors que les fonctions de contrôle d'intégrité peuvent avoir ou non un caractère cryptographique, ceci, selon les besoins de l'utilisateur. A l'émission, l'encapsulation est réalisée par l'entité émettrice après l'exécution de toutes

les fonctions de traitement protocolaires décrites dans la Rec. UIT-T X.224 | ISO/CEI 8073 ou dans la Rec. UIT-T X.234 | ISO 8602, exception faite du multiplexage et de l'affectation de la connexion de réseau. La désencapsulation est effectuée par l'entité réceptrice après démultiplexage et avant toute autre fonction de traitement protocolaire.

5.6.1 Fonction de codage des données

Le codage est un mécanisme qui assure la confidentialité des données. Chaque unité d'encapsulation de sécurité SE TPDU contient une information autonome en ce sens que son décodage ne nécessite la connaissance d'aucune autre SE TPDU. Cette information inclut l'identification des attributs d'association de sécurité (SA-ID) à utiliser pour le décodage ainsi que toute éventuelle séquence de synchronisation ou d'initialisation d'algorithme de chiffrement.

5.6.2 Fonction d'intégrité

Cette fonction prend en charge le contrôle d'intégrité des données et l'authentification de leur origine en mode avec ou sans connexion. Les facteurs d'intégrité et les mécanismes utilisés pour les contrôler sont les suivants:

Protection contre	Mécanisme	CBTSS connexion	GTSS sans connexion
Modification	Valeur ICV calculée pour l'en-tête protégé et la PDU encapsulée	x	x
Insertion	Valeur ICV et numéros de séquence de transport	x	
Suppression	Valeur ICV et numéros de séquence de transport	x	
Repassage de l'enregistrement d'une connexion	Clé distincte pour chaque connexion de transport (Kg_tc) ou identificateur de connexion unique sous chaque clé	x	
Repassage de l'enregistrement d'une PDU	Clé distincte pour chaque connexion de transport (Kg_tc) avec numéros de séquence uniques sous chaque clé, ou identificateur de connexion et numéro de séquence uniques sous chaque clé	x	
Réflexion	Indicateur de direction (champ de drapeaux) dans chaque SE TPDU	x	x
Usurpation	Valeur ICV et, clé de contrôle d'intégrité ou de codage, unique pour une adresse de transport	x	

5.6.3 Fonction d'étiquetage de sécurité

L'étiquetage de sécurité est une fonction optionnelle qui peut être utilisée pour associer une étiquette de sécurité à chaque TPDU encapsulée. L'étiquette signale la sensibilité des données. L'étiquette de sécurité prend en charge les mécanismes de contrôle d'accès.

La structure et l'interprétation du contenu de l'étiquette sont définis par diverses autorités définissantes. L'autorité définissante est identifiée par un identificateur d'objet, codé comme une définition de contenu, comme le spécifie la Rec. X.209 du CCITT | ISO/CEI 8825.

5.6.4 Fonction de remplissage de sécurité

Le remplissage de sécurité est une fonction optionnelle servant à étendre la longueur d'une TPDU encapsulée selon les besoins. Ceci permet de répondre aux spécifications de l'algorithme cryptographique tant pour la confidentialité que pour l'intégrité.

5.6.5 Fonction d'authentification d'entité homologue

Cette fonction procède à l'authentification de l'entité homologue par un échange de PDU encapsulées d'établissement de connexion, contenant un identificateur de connexion comme l'illustre la Figure 3.

Les références de source et de destination doivent:

- avoir une protection d'intégrité; et
- être uniques sur toute la durée de vie de la clé d'intégrité.

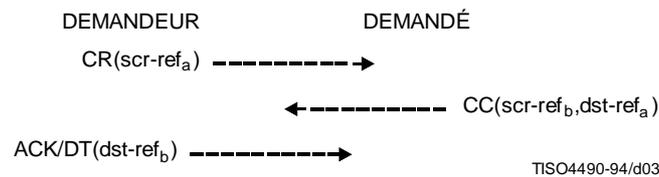


Figure 3 – Primitives échangées par les entités homologues aux fins d'authentification

5.6.6 Fonction SA utilisant le protocole SA-P dans la bande

Ce protocole peut être initialisé à l'aide des procédures définies dans la Rec. UIT-T X.224 | ISO/CEI 8073 pour assurer le transfert de SA-P PDU mais cette initialisation doit s'effectuer avant l'établissement de la connexion de transport ou par l'intermédiaire de la gestion locale. Si les procédures définies dans la Rec. UIT-T X.224 | ISO/CEI 8073 sont mises en œuvre, un numéro de référence local doit être utilisé pour indiquer sans ambiguïté que cette fonction est applicable dans la couche transport pour l'établissement, le maintien et la libération de l'association SA.

NOTE – Si les systèmes qui mettent en œuvre la Rec. UIT-T X.234 | ISO 8602 estiment que le niveau de fiabilité associé à l'établissement d'une association de sécurité n'est pas accessible, ils peuvent décider de ne pas utiliser la méthode du protocole SA-P dans la bande pour établir une association de sécurité.

6 Éléments de procédure

Les éléments de procédure sont ceux qui sont spécifiés dans la spécification du protocole de transport en mode connexion (voir la Rec. UIT-T X.224 | ISO/CEI 8073) et dans le protocole pour fournir un service de transport en mode sans connexion (voir la Rec. UIT-T X.234 | ISO 8602) avec les éléments complémentaires suivants.

Les mécanismes protocolaires suivants servent à l'encapsulation des données. Une TPDU d'encapsulation de sécurité (SE TPDU) comprend:

- a) un en-tête en clair;
- b) un en-tête protégé, avec les champs de longueur et de fanions; si la fonction de confidentialité n'est pas utilisée, cet en-tête est également en clair;
- c) une TPDU unique ou un ensemble de TPDU concaténées conformément aux règles établies par la Rec. UIT-T X.224 | ISO/CEI 8073;
- d) un champ de paramètre ICV si la fonction de contrôle d'intégrité est utilisée;
- e) des champs de remplissage selon les besoins des fonctions d'intégrité et de confidentialité;
- f) une étiquette de sécurité, si le mécanisme d'étiquetage est utilisé.

Une TPDU sera protégée sur la base des attributs de l'association de sécurité, et encapsulée dans une unité d'encapsulation SE TPDU. A la réception d'une SE TPDU, l'entité de transport vérifiera que toutes les protections spécifiées par les attributs de l'association de sécurité existent bien. Toute TPDU incorrectement protégée (qui n'est pas protégée conformément aux attributs de l'association de sécurité) sera éliminée.

NOTE – La réception de telles TPDU incorrectement protégées est un événement qui relève de la sécurité; la suite à donner à un tel événement (établir un rapport de vérification par exemple) sort toutefois du cadre de la présente Recommandation | Norme internationale.

Si la fonction d'encapsulation de sécurité est appelée pour une TPDU pour laquelle il n'existe pas d'association de sécurité correspondante, le protocole de sécurité TLSP pourra soit lancer un protocole d'établissement d'association de sécurité comme spécifié dans la présente Recommandation | Norme internationale soit prendre une autre mesure appropriée.

6.1 Concaténation et séparation

La procédure de concaténation et de séparation est celle qui est spécifiée au 6.4 de la spécification du protocole de transport en mode connexion (voir la Rec. UIT-T X.224 | ISO/CEI 8073), avec les modifications suivantes:

- a) la concaténation ne pourra avoir lieu qu'avant l'encapsulation. Toute TPDU définie dans la Rec. UIT-T X.224 | ISO/CEI 8073 peut être transférée après avoir été encapsulée dans une unité d'encapsulation SE TPDU. Ne pourront être concaténées que des TPDU à protéger par la même clé d'association de sécurité;
- b) une unité d'encapsulation SE TPDU ne sera jamais encapsulée dans une autre unité d'encapsulation SE TPDU.

NOTE – Cette procédure n'est pas utilisée dans le protocole de transport en mode sans connexion (Rec. UIT-T X.234 | ISO 8602).

6.2 Confidentialité

6.2.1 Objet

La confidentialité peut être utilisée par le protocole de transport en mode avec ou sans connexion pour la protection de bout en bout des TPDU et des informations de contrôle de sécurité transitant entre deux entités de transport en communication.

6.2.2 TPDU et paramètres utilisés

La procédure utilise la TPDU et les paramètres suivants:

- SE TPDU (unité de données d'encapsulation);
- SA-ID (identificateur d'association de sécurité);
- Crypto-synch (synchronisation cryptographique);
- Encipherment Pad (remplissage de codage).

6.2.3 Procédure

Si la confidentialité est spécifiée pour une association de sécurité (Conf = vrai), alors toutes les TPDU seront protégées par encapsulation dans une unité d'encapsulation SE TPDU. Tous les octets venant à la suite de l'identificateur SA-ID (l'en-tête protégé et les TPDU) seront codés (voir la Figure 4). Si l'algorithme de codage nécessite un champ de synchronisation cryptographique, ce champ sera positionné avant le contenu protégé et après l'en-tête en clair.

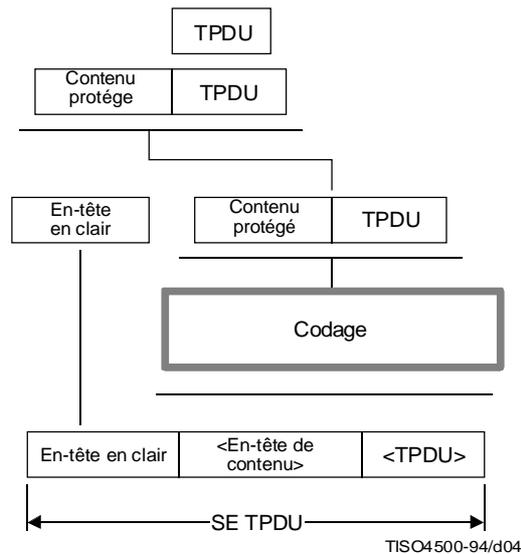
Avant le codage, la fin de l'unité d'encapsulation recevra si nécessaire un remplissage de codage de telle sorte que la longueur du contenu protégé (y compris le champ de longueur de contenu protégé) plus la longueur de la variable de contrôle d'intégrité ICV et le champ de remplissage du contrôle ICV (si la fonction d'intégrité est mise en œuvre) plus la longueur du remplissage de codage représente un multiple entier de la taille de bloc de codage (attribut Enc_Blk de l'association de sécurité). A la réception, le champ de synchronisation cryptographique sera utilisé s'il est présent aux fins de synchronisation.

L'algorithme cryptographique est spécifié par un attribut de l'association de sécurité qui est identifié par l'identificateur d'association de sécurité SA-ID.

Lorsqu'elle reçoit une unité d'encapsulation SE TPDU, l'entité de transport utilise la clé de codage identifiée par l'identificateur SA-ID dans cette SE TPDU pour identifier le service de sécurité et décoder la SE TPDU. Le contenu du champ de remplissage de codage sera ignoré à la réception. Si la clé n'est pas trouvée, la SE TPDU est ignorée.

NOTE – La réception d'une SE TPDU ayant un identificateur d'association de sécurité SA-ID non valide est un événement qui relève de la sécurité; la suite à donner à un tel événement (établir un rapport de vérification par exemple) sort toutefois du cadre de la présente Recommandation | Norme internationale.

Traitement assurant la fonction de confidentialité



NOTE – Les quantités entre parenthèses sont codées.

Figure 4 – Méthodes d'encapsulation du protocole TLS (Méthode d'encapsulation et de codage assurant la fonction de confidentialité comme indiqué au 6.2)

6.3 Procédure d'intégrité

Les procédures suivantes sont utilisées pour assurer les services d'intégrité en mode avec ou sans connexion.

6.3.1 Traitement de la valeur de contrôle d'intégrité (ICV)

6.3.1.1 Objet

Le traitement de la valeur ICV peut être utilisé par le protocole de sécurité de la couche transport TLS tant en mode connexion (Rec. UIT-T X.224 | ISO/CEI 8073) qu'en mode sans connexion (Rec. UIT-T X.234 | ISO 8602), pour détecter une altération non autorisée des données d'utilisateur et de l'information de contrôle de sécurité pendant que celles-ci transitent entre les entités de transport en communication.

6.3.1.2 TPDU et paramètres utilisés

La procédure utilise la TPDU et les paramètres suivants:

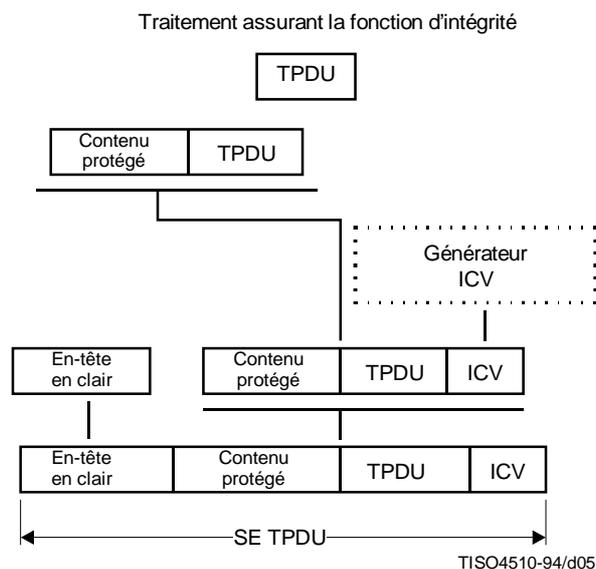
- SE TPDU (unité de données d'encapsulation);
- SA-ID (identificateur d'association de sécurité);
- Integrity PAD (remplissage d'intégrité);
- ICV (valeur de contrôle d'intégrité).

6.3.1.3 Procédure

Il existe deux types de traitement de contrôle d'intégrité: le code d'authentification de message (MAC) (*message authentication code*) et le code de détection de manipulation (MDC) (*manipulation detection code*). L'utilisation du code MAC ou MDC dépend directement de ce qui est spécifié: intégrité seule ou intégrité et confidentialité. Si l'intégrité

seule est choisie, c'est un code MAC à chiffrement qui sera utilisé. Si l'intégrité et la confidentialité sont toutes deux spécifiées, le contrôle ICV peut être assuré soit par un code de détection de manipulation (MDC) sans chiffrement (par fonction XOR ou par contrôle de somme par exemple), soit par un moyen avec chiffrement (le code MAC par exemple). Il n'est pas nécessaire de recourir au chiffrement car le contenu protégé sera chiffré dans son entier, puisque la confidentialité a également été spécifiée. Si la confidentialité a seule été spécifiée, il n'y aura pas de champ ICV.

Si l'intégrité des données a été spécifiée (Integ = vrai) pour une association cryptographique, chaque unité d'encapsulation SE TPDU sera protégée par une valeur de contrôle ICV. Le code d'authentification de message (MAC) véhiculé par le paramètre ICV sera inscrit dans le dernier champ de l'unité d'encapsulation SE TPDU. La valeur de contrôle d'intégrité ICV est calculée pour l'ensemble de l'en-tête protégé et de la TPDU encapsulée. Si en plus de l'intégrité, la confidentialité a été spécifiée (Conf = vrai), le code de détection de manipulation (MDC) ou le code MAC à chiffrement est calculé avant codage. Un remplissage d'intégrité complètera si nécessaire le contenu protégé de façon à ce que la longueur du contenu protégé (y compris le champ de contenu protégé) soit un multiple entier de la taille de bloc ICV (attribut ICV_Blck de l'association de sécurité). Le contenu du champ de remplissage d'intégrité sera ignoré à la réception. Voir la Figure 5.



**Figure 5 – Méthodes d'encapsulation du protocole TLSP
(Méthode d'encapsulation et de génération de valeur de contrôle d'intégrité
assurant la fonction d'intégrité comme indiqué au 6.3)**

La fonction de contrôle d'intégrité (ICV) et la longueur du champ ICV sont des attributs de l'association de sécurité.

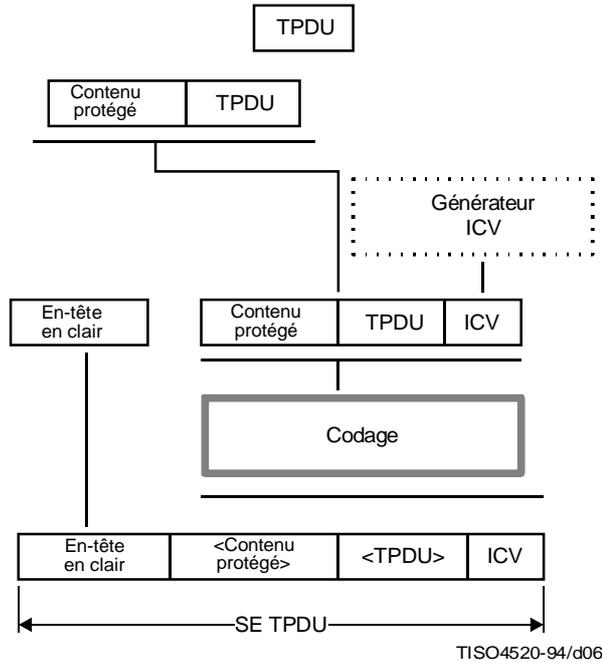
Lorsqu'une unité d'encapsulation SE TPDU dotée de la protection d'intégrité est reçue sur une association de sécurité, le champ ICV sera contrôlé en calculant une valeur ICV de vérification sur l'ensemble de l'en-tête protégé et de la TPDU encapsulée. Si l'association de sécurité identifiée par l'identificateur SA-ID n'est pas disponible ou si la valeur ICV de vérification n'est pas égale à la valeur contenue dans le champ ICV, l'unité d'encapsulation SE TPDU est ignorée dans son ensemble.

NOTE – L'échec du contrôle ICV est un événement qui relève de la sécurité; la suite à donner à un tel événement (établir un rapport de vérification par exemple) sort toutefois du cadre de la présente Recommandation | Norme internationale.

Si le codage est également spécifié, la vérification de la valeur ICV sera effectuée après décodage.

La Figure 6 décrit l'intégrité et la confidentialité.

Traitement assurant la fonction d'intégrité et de confidentialité



NOTE – Les quantités entre parenthèses sont codées.

**Figure 6 – Méthodes d'encapsulation du protocole TLSP
(Méthode d'encapsulation et de génération de valeur de contrôle d'intégrité
assurant la fonction d'«intégrité» et de «confidentialité» comme indiqué aux 6.2 et 6.3)**

6.3.2 Traitement de l'indicateur de direction

6.3.2.1 Objet

L'objet de l'indicateur de direction est d'assurer une protection contre les réflexions.

6.3.2.2 TPDU et paramètres utilisés

La procédure utilise la TPDU et les paramètres suivants:

- SE TPDU (unité de données d'encapsulation);
- FLAGS (fanions).

6.3.2.3 Procédure

Chaque unité d'encapsulation SE TPDU comportera un bit indicateur de direction (champ FLAGS) indiquant l'expéditeur de la TPDU. Les parties intervenant dans l'association de sécurité auront déjà décidé de qui était le demandeur et qui était le demandeur de l'association. Lorsqu'une unité d'encapsulation SE TPDU est expédiée par le demandeur de l'association de sécurité, le bit indicateur de direction sera mis à 1. Lorsqu'une unité d'encapsulation SE TPDU est expédiée par le demandé de l'association de sécurité, le bit indicateur de direction sera mis à 0. Lors de la réception d'une unité d'encapsulation SE TPDU, l'entité de transport validera le bit indicateur de direction. Si l'indicateur de direction reçu est incorrect, l'unité d'encapsulation SE TPDU est ignorée.

NOTE – La réception d'une unité de données d'encapsulation SE TPDU ayant un indicateur de direction incorrect est un événement qui relève de la sécurité; la suite à donner à un tel événement (établir un rapport de vérification par exemple) sort toutefois du cadre de la présente Recommandation | Norme internationale.

6.3.3 Traitement du numéro de séquence d'intégrité de connexion

La détection du repassage d'enregistrement, de l'insertion et de la suppression nécessite d'attribuer à chaque TPDU échangée par une association de sécurité un numéro de séquence unique. Lorsque la fonction d'intégrité en mode connexion a été spécifiée pour une connexion donnée (Kg_{tc} = clé distincte pour chaque connexion; $Integ_yes$ = intégrité à assurer), elle sera assurée en utilisant une clé par connexion en même temps qu'une procédure d'attribution de numéro de séquence unique (voir 6.3.3.1). Cette procédure n'est pas utilisée dans le cadre de la Rec. UIT-T X.234 | ISO 8602.

6.3.3.1 Numéros de séquence uniques

Les numéros de séquence uniques sont ceux qui sont mentionnés dans la Rec. UIT-T X.224 | ISO/CEI 8073 (voir 6.10 et 6.11).

6.3.3.2 Objet

L'attribution de numéros de séquence uniques est une procédure optionnelle destinée à identifier de manière unique chaque unité de données normales (TPDU DT) ou de données exprès (TPDU ED) sur une connexion particulière. Cette procédure n'est applicable que dans le cadre de la Rec. UIT-T X.224 | ISO/CEI 8073 (classes 2, 3 et 4).

6.3.3.3 Procédure

Lorsque le service d'intégrité en mode connexion est spécifié pour une connexion de transport (Kg_{tc} et $Integ$ = vrai), chaque unité de données TPDU se verra attribuer un numéro de séquence unique pour l'association de sécurité. Aucune des deux entités de transport n'expédiera d'unité de données normales (TPDU DT) ou exprès (TPDU ED) avec un numéro de séquence déjà utilisé avec la même clé. La retransmission des TPDU dans le cadre normal de la reprise et de la correction d'erreur peut reprendre le même numéro de séquence avec la clé d'origine ou utiliser une nouvelle clé. Lorsque l'espace prévu pour le numéro de séquence des données normales ou exprès est saturé sur une connexion particulière, il est possible de choisir une clé cryptographique différente de toutes celles précédemment utilisées avec le même identificateur de connexion (DST-REF) afin de transmettre de nouvelles TPDU. La procédure de remplacement de clé (voir 6.7) sera appelée. Si une telle clé n'existe pas, la connexion peut être libérée. Si une TPDU de données normales ou exprès est reçue avec un numéro de séquence déjà paru sous la même clé cryptographique, elle sera ignorée par l'entité de transport.

NOTE – La réception d'une TPDU de données normales ou exprès avec un numéro de séquence déjà paru est un événement qui relève de la sécurité; la suite à donner à un tel événement (établir un rapport de vérification par exemple) sort toutefois du cadre de la présente Recommandation | Norme internationale.

Le numéro de séquence unique est le numéro de séquence de transport utilisé dans les classes 2, 3, et 4. Il est recommandé d'utiliser les numéros de séquence étendus pour éviter la redéfinition de clé.

6.4 Traitement de la vérification d'adresse d'homologue

6.4.1 Objet

Cette procédure a pour but de contrer les actes de piraterie par usurpation et d'assurer l'authentification de l'origine des données.

6.4.2 Procédure

Lors de la réception d'une TPDU, l'adresse d'homologue associée à la clé cryptographique sera comparée avec l'adresse de source de la TPDU. Si ces adresses ne concordent pas, l'unité d'encapsulation SE TPDU sera ignorée.

NOTE – La réception d'une unité d'encapsulation SE TPDU avec une adresse non valide est un événement qui relève de la sécurité; la suite à donner à un tel événement (établir un rapport de vérification par exemple) sort toutefois du cadre de la présente Recommandation | Norme internationale.

A chaque granularité de clé correspond un niveau d'information d'adresse homologue à vérifier. Lorsqu'un chiffrement à une clé par système terminal (Kg_{esp}) est utilisé, l'adresse de point d'accès au service réseau (NSAP) de l'entité de transport homologue est vérifiée par comparaison avec l'adresse d'homologue négociée. Lorsqu'un chiffrement à une clé par système terminal et par niveau de sécurité (Kg_{esp_sr}) est utilisé, l'étiquette de sécurité de l'unité d'encapsulation SE TPDU est vérifiée par comparaison avec le niveau de sécurité négocié, en plus de la vérification de l'adresse de point NSAP de l'entité de transport homologue. Comme l'étiquette de sécurité n'est pas à proprement parler une information d'adresse et que son utilisation est optionnelle dans les associations de sécurité à niveau simple, elle est vérifiée indépendamment comme cela est indiqué par ailleurs (voir 6.5, étiquettes de sécurité pour les associations de sécurité).

Lorsqu'un chiffrement à une clé par connexion (K_{g_tc}) est utilisé, la procédure devient un peu plus complexe, car, en plus de l'adresse de point NSAP de l'entité de transport homologue, il faut vérifier les identificateurs de connexion de transport (SRC-REF et DST-REF) véhiculés par chacune des TPDU. L'identificateur SRC-REF est vérifié par comparaison avec la partie de l'attribut de sécurité de l'adresse homologue correspondant au numéro de référence de l'entité de transport distante, et l'identificateur DST-REF par comparaison avec la référence locale de la connexion. A noter que l'entité de transport qui demande une connexion peut ne pas connaître la référence locale utilisée par l'entité homologue, et peut donc ne pas pouvoir vérifier l'identificateur SRC-REF d'une unité de confirmation de connexion (TPDU CC). Une telle situation se produit lorsque l'entité homologue détermine dynamiquement la référence locale lors du traitement d'une unité de demande de connexion (TPDU CR), et que le gestionnaire des clés de chiffrement ne dispose d'aucune valeur à transmettre au moment où les attributs de sécurité sont choisis. La TPDU peut être acceptée et la valeur du champ d'identificateur SRC-REF retenue, sous réserve que le champ d'identificateur DST-REF de l'unité de confirmation de connexion TPDU CC porte la même valeur que la référence locale de la connexion.

6.5 Étiquettes de sécurité des associations de sécurité

6.5.1 Objet

Les étiquettes de sécurité sont utilisées comme moyen support du contrôle d'accès et comme moyen support pour la séparation des données en fonction de leur sensibilité.

6.5.2 TPDU et paramètres utilisés

La procédure utilise la TPDU et les paramètres suivants:

- SE TPDU (unité de données d'encapsulation);
- SA-ID (identificateur d'association de sécurité);
- LABEL (étiquette).

6.5.3 Procédure

S'il est spécifié pour l'association de sécurité d'utiliser une étiquette de sécurité explicite pour chaque TPDU, cette étiquette sera inscrite dans le champ LABEL (étiquette) de l'en-tête protégé de chaque unité d'encapsulation SE TPDU. Lors de la réception d'une unité d'encapsulation SE TPDU étiquetée, l'entité de transport s'assurera que le paramètre LABEL appartient à l'ensemble des niveaux de sécurité acceptables pour l'association de sécurité. Si l'étiquette LABEL de l'unité d'encapsulation SE TPDU reçue n'est pas valable, la TPDU sera ignorée.

NOTE – La réception d'une unité d'encapsulation SE TPDU avec une étiquette impropre est un événement qui relève de la sécurité; la suite à donner à un tel événement (établir un rapport de vérification par exemple) sort toutefois du cadre de la présente Recommandation | Norme internationale.

6.6 Libération de la connexion

Si c'est le service orienté connexion (K_{g_tc}) qui est utilisé, la clé associée à la connexion sera désélectionnée dans le cadre de la procédure de libération de la connexion.

6.7 Remplacement de clé

La procédure de remplacement de clé est exécutée à l'expiration de la période cryptographique correspondante. Si le service utilisé est orienté connexion (K_{g_tc}), la procédure peut également être appliquée après saturation du champ prévu pour les numéros de séquence (voir 6.3.3.1).

La procédure de remplacement de clé associe une nouvelle clé cryptographique à une ou plusieurs connexions de transport actives. Les attributs de la nouvelle association de sécurité seront identiques à ceux de l'ancienne sauf pour ce qui est de la nouvelle clé. S'il n'existe pas de telle clé, l'entité de gestion de la sécurité en sera informée, et l'ancienne clé cryptographique ne sera pas utilisée pour la transmission. Une fois la procédure de remplacement de clé exécutée, l'ancienne clé cryptographique sera supprimée. L'inexistence de nouvelle clé appropriée est un événement qui relève de la sécurité; la suite à donner à un tel événement (établir un rapport de vérification par exemple) relève toutefois d'un choix local.

NOTE – La nouvelle clé doit être instituée avant expiration de la temporisation d'activité de transport (pour la classe 4) ou de la temporisation TWR (classe 3), faute de quoi le protocole de transport peut mettre fin à la connexion.

Une fois la clé remplacée, des TPDU de données normales ou exprès sans acquittement demandant la reprise de la transmission seront échangées sous la nouvelle clé.

6.8 TPDU non protégées

La politique de sécurité peut prévoir l'établissement de connexions de transport sûres et non sûres entre deux entités de communication. Un tel choix relève de la compétence locale.

Si à l'émission, l'attribut de l'association de sécurité UNProt (non protégé) à la valeur vrai, la TPDU est passée en transparence par le protocole de sécurité TLSP, sans protection ni traitement.

Si à la réception, l'attribut de l'association de sécurité UNProt (non protégé) à la valeur vrai, la TPDU reçue est passée en transparence sans être soumise aux procédures du protocole de sécurité TLSP.

6.9 Identification du protocole

Si ce protocole est utilisé sur une connexion de réseau, il sera identifié explicitement par les procédures d'identification explicite définies dans ISO/CEI 11570. La TPDU d'utilisation de connexion de réseau (TPDU UN) peut être elle-même protégée par le protocole spécifié dans la présente Recommandation | Norme internationale. Si la TPDU UN n'est pas protégée et si elle spécifie la présente Recommandation | Norme internationale en même temps que la Rec. UIT-T X.224 | ISO/CEI 8073 ou que la Rec. UIT-T X.234 | ISO 8602, la protection des TPDU sera assurée conformément aux attributs de l'association de sécurité une fois la connexion de réseau établie. Si la TPDU UN est protégée et si elle spécifie la Rec. UIT-T X.224 | ISO/CEI 8073 seule ou la Rec. UIT-T X.234 | ISO 8602 seule, alors le protocole spécifié est seul utilisé une fois la connexion de réseau établie.

NOTES

- 1 La prise en charge ou non de la communication non protégée dépend des attributs de l'association de sécurité.
- 2 Si les connexions de transport sont prises en charge, la possibilité de les multiplexer ou non avec des connexions de transport protégées sur la même connexion de réseau dépend des attributs de l'association de sécurité et de la politique de sécurité de l'entité concernée.

La procédure d'identification explicite définie dans ISO/CEI 11570 n'est pas utilisée si la Rec. UIT-T X.224 | ISO/CEI 8073 (classe 4) est mise en œuvre sur un service réseau OSI en mode sans connexion, comme cela est défini dans ISO 8348.

6.10 Protocole d'association de sécurité

Un protocole d'association de sécurité (SA-P) est mis en œuvre par l'échange de SA PDU pour permettre l'établissement et la personnalisation d'une association SA.

Les champs exacts inclus dans les SA PDU utilisées pour l'échange d'informations de sécurité dépendent du mécanisme spécifique qui doit être mis en œuvre pour établir l'association SA. Quel que soit le mécanisme utilisé pour le protocole SA-P, il doit assurer les fonctions suivantes:

- a) calcul de tous les attributs SA nécessaires pour la forme de protection sélectionnée;
- b) authentification des clés calculées;
- c) établissement d'informations initiales à des fins d'authentification et, si nécessaire, d'intégrité;
- d) modification des clés;
- e) libération de l'association de sécurité.

Un algorithme symétrique ou asymétrique peut être utilisé pour ces fonctions. Il est recommandé d'utiliser un algorithme asymétrique. L'Annexe B contient un exemple d'un tel mécanisme.

Pendant la partie de l'établissement d'une association SA qui nécessite un échange d'informations sous une forme non protégée, il convient d'utiliser des SA PDU. Les échanges d'informations protégées nécessaires pour l'établissement de l'association SA peuvent être effectués dans des SA PDU ou SE TPDU.

Immédiatement après la réception de la dernière SA PDU dans le protocole SA-P, si une TPDU attend un encapsulage de sécurité, elle est traitée et transmise.

NOTE – Il est nécessaire que la dernière SA PDU contenant des informations de commande de sécurité positionne le marqueur de direction à la valeur entité appelée vers entité appelante dans le protocole SA-P. Si nécessaire, une SA PDU ne contenant que les identificateurs SA-ID local et SA-ID homologue peut être envoyée.

Si la séquence de PDU prévue n'apparaît pas dans un délai de temporisation spécifié, une SA PDU utilisée pour l'échange d'informations de commande de sécurité (SCI) peut être répétée plusieurs fois. La réception SA PDU contenant des informations SCI précédemment reçues entraînera le renvoi des SA PDU précédemment envoyées en réponse. Les SA PDU contenant des informations SCI qui sont en dehors de la séquence prévue doivent être ignorées.

Une entité TSLP peut abandonner une procédure d'établissement d'association SA et ignorer les SA PDU ultérieures contenant des informations SCI en cas d'échec d'un quelconque test de vérification.

7 Utilisation des éléments de procédure

Le Tableau 1 donne une vue d'ensemble des éléments de procédure à inclure dans chacune des classes du protocole de la Rec. UIT-T X.224 | ISO/CEI 8073 et dans le protocole de la Rec. UIT-T X.234 | ISO 8602.

Tableau 1 – Eléments de procédure du protocole de sécurité TLSP

Mécanisme protocolaire	Référence (paragraphe)	Rec. UIT-T X.224 ISO/CEI 8073, Classe					Rec. UIT-T X.234 ISO 8602
		m	m	m	m	m	
Confidentialité cryptographique	6.2	m	m	m	m	m	m
Traitement ICV	6.3.1	m	m	m	m	m	m
Traitement d'indicateur de direction	6.3.2	*	*	*	*	*	*
Numéros de séquence uniques	6.3.3.1	NA	NA	o	o	o	NA
Traitement de vérification d'adresse d'homologue	6.4	*	*	*	*	*	*
Etiquettes de sécurité pour association cryptographique	6.5	o	o	o	o	o	o
Libération de connexion	6.6	o	o	o	o	o	NA
Remplacement de clé cryptographique	6.7	o	o	o	o	o	o
<p>* Procédure toujours incluse dans la classe. NA Non applicable. o Procédure négociable et dont la programmation dans l'équipement est facultative (<i>optional</i>). m Procédure négociable et dont la programmation dans l'équipement est obligatoire (<i>mandatory</i>). NOTE – La négociation de ces éléments sort actuellement du cadre de la présente Recommandation Norme internationale, mais la procédure SA-P décrite au 6.10 permet de procéder à cette négociation dans le cadre du protocole TLSP à tout moment avant l'établissement de la connexion.</p>							

8 Structure et codage des TPDU

8.1 Structure de la TPDU

La structure de la TPDU (ou des TPDU concaténées) avant encapsulation (c'est-à-dire avant d'être placées dans le champ «données protégées» d'une unité d'encapsulation SE TPDU, voir 8.2) est définie au 13.2 de la Rec. UIT-T X.224 | ISO/CEI 8073.

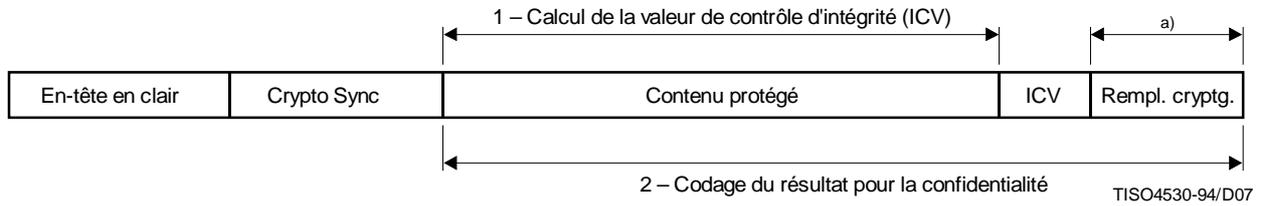
8.2 Unité d'encapsulation de sécurité TPDU

Toutes les unités d'encapsulation SE TPDU comprendront un nombre entier d'octets. Les octets d'une SE TPDU sont numérotés à partir de 1 en ordre croissant dans l'ordre où ils sont insérés dans l'unité de données du service réseau (NSDU). Les bits de chaque octet sont numérotés de 1 à 8, le bit 1 ayant le poids le plus faible.

Lorsque des octets consécutifs appartenant à une même unité d'encapsulation SE TPDU sont utilisés pour représenter un nombre binaire, l'octet ayant le numéro le plus petit aura la valeur la plus significative.

Dans les figures suivantes, le nombre d'octets des champs de longueur fixe de l'unité d'encapsulation SE TPDU est indiqué en dessous de chacun de ces champs.

La structure de l'unité d'encapsulation SE TPDU est la suivante:



a) La présence de ce champ dépend du fait que l'algorithme de codage nécessite ou non un remplissage de codage indépendant.

Figure 7 – Structure de la TPDU

8.2.1 En-tête en clair

Voir la Figure 8.

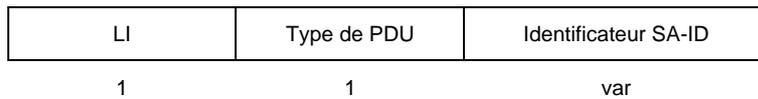


Figure 8 – Format de l'en-tête en clair

8.2.1.1 Longueur de l'en-tête en clair de la PDU

Le champ de l'indicateur de longueur (LI) de l'en-tête en clair de la PDU contient la longueur en octets des champs type de PDU et identificateur SA-ID, non compris la longueur du champ LI lui-même.

8.2.1.2 Type de PDU

Ce champ contient le code PDU TYPE. Il est utilisé pour définir la structure du reste de l'en-tête. La valeur du code PDU TYPE est 0100 1000.

8.2.1.3 Identificateur SA-ID

Le champ de l'identificateur de l'association de sécurité (SA-ID) contient l'identificateur distant de la clé cryptographique utilisée pour protéger la TPDU.

8.2.2 Synchronisation cryptographique

Il s'agit d'un champ optionnel pouvant contenir les données de synchronisation propres à l'algorithme de codage identifié par les attributs de l'association de sécurité.

NOTE – La taille de ce champ serait connue des entités communicantes et ferait partie des attributs de l'association.

8.2.3 Contenu protégé

La Figure 9 illustre le format du contenu protégé des PDU de sécurité.

Longueur du contenu	Flags	Label	Données protégées	Remplissage d'intégrité
1-3	1	(tlv)	(tlv)	(tlv) ^{a)}

a) Il peut s'agir d'un remplissage à un seul octet.

Figure 9 – Contenu protégé

8.2.3.1 Structure des champs du contenu protégé

Les différents champs du contenu protégé sont codés en type, longueur et valeur (codage tlv).

Le champ de type de contenu peut recevoir les valeurs suivantes:

Valeur	Type de contenu
00-7F	Réservé pour utilisation privée
80-BF	Réservé
C0	Données protégées
C1-C5	Réservé
C6	Etiquette
C7-CF	Réservé
D0	Réservé
D1	Remplissage à un seul octet
D2	Réservé
D3	Remplissage d'intégrité
D4	Remplissage de codage
D5-FF	Réservé pour utilisation future

Si le remplissage d'intégrité ou de codage nécessite un champ à deux octets, le champ de longueur prendra la valeur 0 avec le type de champ de contenu approprié.

Le champ de longueur de contenu contient la longueur en octets de la valeur du champ de contenu; il peut comporter un, deux ou trois octets:

- a) s'il ne comporte qu'un octet, le bit 8 contient le chiffre 0, et les 7 autres bits définissent une longueur de champ allant jusqu'à 127 octets.
- b) s'il comporte deux octets, le premier est codé 1000 0001 et le second octet définit une longueur de champ allant jusqu'à 255 octets.
- c) s'il comporte trois octets, le premier est codé 1000 0010 et les deux octets suivants définissent une longueur de champ allant jusqu'à 65 535 octets.

Les autres valeurs pour le premier octet sont réservées pour utilisation future.

8.2.3.2 Champ de longueur du contenu

Le champ de longueur contient la longueur en octets du contenu protégé, non compris le champ de longueur de contenu lui-même (il s'agit donc de la longueur des champs de fanion, d'étiquette, de données protégées et de remplissage d'intégrité). La valeur maximale qu'il puisse prendre est 65 535 (soit $2^{16} - 1$).

8.2.3.3 Champ Flags (fanions)

Voir la Figure 10.

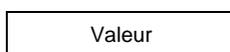


Figure 10 – Champ des fanions (Flags)

Les bits de ce champ actuellement affectés sont les suivants:

- *bit 1: indicateur de direction*
0 = demandé vers demandeur;
1 = demandeur vers demandé;
- *bit 4: envoi/réponse*
0 = envoi;
1 = réponse.

Les bits de fanions inutilisés 2 à 3 et 5 à 8 sont mis à zéro pour la transmission.

8.2.3.4 Champ Label (étiquette)

Voir la Figure 11.

C6 Hex	Longueur étiquette	Longueur autorité de définition	Autorité de définition	Valeur
1	1-3	1-3	var	var

Figure 11 – Format du champ d'étiquette

Le format du champ valeur est spécifié par l'autorité de définition.

NOTE – Il est prévu que ces étiquettes seront enregistrées conformément aux procédures définies par l'ISO et l'UIT-T. Une autorité de définition sera enregistrée comme une valeur d'identificateur d'objet conformément à ISO 8824, codée conformément à ISO 8825 et les procédures utilisées à cet effet seront celles définies dans ISO/CEI 9834.

8.2.3.5 Champ des données protégées

Le champ de données contient une TPDU ou un ensemble de TPDU concaténées, conformément à la Rec. UIT-T X.224 | ISO/CEI 8073 ou à la Rec. UIT-T X.234 | ISO 8602 (voir la Figure 12).

C0 Hex	Longueur	Données protégées
1	var	var

Figure 12 – Format du champ de données protégées

8.2.3.6 Remplissage d'intégrité

Le champ de valeur contient des données arbitraires nécessaires aux mécanismes de contrôle d'intégrité.

La longueur du remplissage est déterminée par:

- a) le remplissage nécessaire au mécanisme d'intégrité.
Le mécanisme d'intégrité utilisé a des caractéristiques connues, et en particulier la longueur de bloc adoptée pour l'association de sécurité (si le mécanisme fonctionne en mode bloc). La longueur totale depuis le point de départ d'application de la procédure de contrôle d'intégrité jusqu'à la fin du remplissage d'intégrité doit être un multiple entier de cette longueur de bloc;
- b) le remplissage nécessaire au mécanisme de codage par bloc afin d'amener la fin du champ ICV sur la fin d'un bloc, lorsqu'un remplissage de codage distinct n'est pas demandé.

Le choix de la valeur de remplissage relève de la compétence locale. Lorsqu'un remplissage à un octet est nécessaire, on utilisera le remplissage à octet simple (Type = D1 – sans valeur ni longueur) à la place du remplissage d'intégrité.

8.2.4 ICV

Le champ ICV contient la valeur de contrôle d'intégrité; sa longueur est déterminée par l'algorithme ICV dont l'identificateur appartient aux attributs de l'association de sécurité.

8.2.5 Remplissage de codage

La taille du bloc de codage est une caractéristique connue de l'algorithme de codage. La longueur totale depuis le point de départ d'application de la procédure de confidentialité jusqu'à la fin du champ ICV doit être un multiple entier de cette longueur de bloc. La présence du remplissage de codage après le champ ICV dépend du fait que l'algorithme de codage choisi nécessite ou non un remplissage de codage distinct.

Le choix de la valeur de remplissage relève de la compétence locale. Lorsqu'un remplissage à un octet est nécessaire, on utilisera le remplissage à octet simple (Type = D1 – sans valeur ni longueur) à la place du remplissage de codage.

8.3 PDU d'association de sécurité

Le format de la SA PDU est indiqué sur la Figure 13.

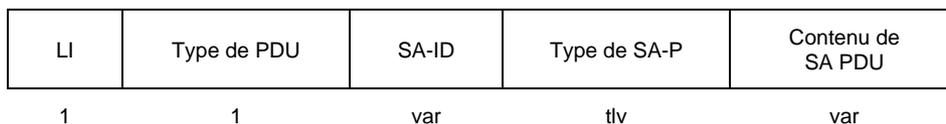


Figure 13 – Structure d'une SA PDU

8.3.1 LI

Ce champ contient la longueur du champ type de PDU et l'identificateur SA-ID. Si une entité doit signaler, dans l'identificateur SA-ID, qu'elle ne connaît pas l'identificateur SA-ID de son entité homologue (par exemple, lors de l'établissement d'une nouvelle association SA), le champ de longueur doit être réglé de telle sorte que le champ SA-ID ne soit pas présent (c'est-à-dire à la valeur 1).

8.3.2 Type de PDU

Ce champ contient le type de PDU, valeur 0100 1001 pour indiquer une PDU d'association de sécurité.

8.3.3 SA-ID

Le champ SA-ID contient l'identificateur d'association de sécurité du destinataire (c'est-à-dire, l'attribut SA Peer_SA-ID). Ce champ n'est pas nécessaire lorsque le protocole SA-P est utilisé pour établir une nouvelle association SA (c'est-à-dire lorsque le destinataire n'a pas encore assigné un identificateur SA-ID).

8.3.4 Type de SA-P

Ce champ contient un identificateur d'objet indiquant le mécanisme établi pour mettre en œuvre le protocole SA; un exemple est donné ci-dessous.

L'identificateur d'objet assigné pour l'échange de clés exponentielles défini dans l'Annexe D est joint-ccitt-iso (2) t1sp (21) sa-p-kte (1) eke (1).

L'utilisation d'autres algorithmes avec le protocole SA-P peut être indiquée par d'autres identificateurs d'objet attribués conformément à ISO 9834-1 (Procédures d'enregistrement).

8.3.5 Contenu de SA PDU

La structure interne de ce champ dépend du mécanisme utilisé pour mettre en œuvre le protocole SA comme indiqué au 8.3.4 ci-dessus. L'Annexe B définit un tel protocole SA fondé sur des mécanismes d'échange de jetons de clé et de signatures numériques.

9 Conformité

9.1 Considérations générales

Pour qu'une instance de protocole puisse prétendre à conformité avec la présente Recommandation | Norme internationale, il faudra remplir une déclaration de conformité d'une instance de protocole (PICS) (*protocol implementation conformance statement*). Cette déclaration PICS sera établie conformément au formulaire PICS approprié.

9.2 Spécifications communes de conformité statique

- a) Une instance conforme mettra en œuvre le protocole TLSP au moins avec le protocole de la Rec. UIT-T X.224 | ISO/CEI 8073 ou celui de la Rec. UIT-T X.234 | ISO 8602.
- b) Une instance conforme mettra en œuvre le protocole dans un système terminal.
- c) Tout système prétendant à conformité avec le protocole TLSP devra pouvoir encapsuler les données utilisateur dans une PDU de transfert sûr de données puis les en extraire.
- d) Tout système prétendant assurer des services de confidentialité devra mettre en œuvre au moins le mécanisme de codage.
- e) Tout système prétendant assurer des services d'intégrité devra mettre en œuvre au moins le mécanisme de valeur de contrôle d'intégrité (ICV).

9.3 Spécifications de conformité statique du protocole TLSP avec le protocole de la Rec. UIT-T X.234 | ISO 8602

Tout système prétendant à conformité avec le protocole TLSP assurera au moins un des services de sécurité suivants:

- a) service de confidentialité en mode sans connexion;
- b) service d'intégrité en mode sans connexion;

9.4 Spécifications de conformité statique du protocole TLSP avec le protocole de la Rec. UIT-T X.224 | ISO/CEI 8073

Tout système prétendant à conformité avec le protocole TLSP assurera au moins un des services de sécurité suivants:

- a) service de confidentialité en mode connexion;
- b) service d'intégrité sans reprise en mode connexion;
- c) authentification de l'entité homologue.

9.5 Spécifications communes de conformité dynamique

Tout système prétendant à conformité avec la présente Recommandation | Norme internationale présentera le comportement suivant:

- a) détection de tous les champs obligatoires et optionnels pouvant apparaître dans une PDU de transfert sûr de données;
- b) les champs non reconnus dans une PDU de transfert sûr de données seront traités comme des erreurs, comme cela est décrit dans l'article 6.

9.6 Spécifications de conformité dynamique du protocole TLSP avec le protocole de la Rec. UIT-T X.234 | ISO 8602

Tout système prétendant à conformité avec le protocole TLSP présentera le comportement suivant:

- si le service d'authentification de l'origine des données est assuré, il sera fait appel soit au mécanisme de codage, soit au mécanisme d'intégrité ICV cryptographique.

9.7 Spécifications de conformité dynamique du protocole TLSP avec le protocole de la Rec. UIT-T X.224 | ISO/CEI 8073

Tout système prétendant à conformité avec le protocole TLSP présentera le comportement suivant:

- si le service d'authentification de l'entité homologue ou de l'origine des données est assuré, il sera fait appel soit au mécanisme de codage, soit au mécanisme d'intégrité ICV cryptographique.

10 Déclaration de conformité d'une instance de protocole (PICS)

Le fournisseur d'une instance de protocole prétendue conforme à la présente Recommandation | Norme internationale devra remplir un exemplaire du formulaire PICS fourni en Annexe A, et fournir les informations nécessaires à l'identification tant du fournisseur que de l'instance de protocole.

Annexe A

Formulaire PICS^{a)}

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

A.1 Introduction

A.1.1 Background

The supplier of a protocol implementation which is claimed to conform to Recommendation | International Standard 10736 shall complete the Transport Layer Security Protocol (TLSP), Protocol Implementation Conformance Statement (PICS) proforma. A completed PICS proforma becomes the PICS for the implementation in question. The PICS is a statement identifying the capabilities and options of the protocol that have been implemented. The PICS can have a number of uses, including:

- use by the protocol implementer, as a check list to reduce the risk of failure to conform to the standard through oversight;
- use by the supplier and receiver of the implementation, as a detailed indication of its capabilities, stated relative to the common basis of understanding provided by the standard PICS proforma;
- use by the user of the implementation, as a basis for checking the possibility of interworking with another implementation;
- use by a protocol tester, as the basis for selecting appropriate tests against which to assess the claim for conformance of the implementation.

A.1.2 Approach

The first part of the PICS proforma, the Implementation Identification and Protocol Summary, is to be completed as indicated with the information necessary to identify fully both the supplier and the implementation. The main part of the PICS proforma is a fixed-format questionnaire divided into subclauses, each containing a group of individual items. Answers to the questionnaire items are to be provided in the rightmost column, either by simply marking an answer to indicate a restricted choice (usually “Yes” or “No”), or by entering a value or a set or range of values. Note that there are some items where two or more choices from a set of possible answers can apply. Therefore, all relevant choices are to be marked.

Each item is identified by an reference index in the first column; the second column contains the item to be addressed; the third column contains the reference(s) to the location of the item in the main body of the standard. For optional items, additional columns indicate the status of the item (i.e. whether support is mandatory, optional, or conditional), and provide space or a choice or items for the implementation support response.

The following status column notations described in ISO/IEC JTC1/ SC6 N6233, Catalogue of PICS Proforma Notations, are used for this PICS proforma:

<i>Symbol</i>	<i>Meaning</i>
m	Mandatory
o	Optional
–	Not applicable (N/A)
o.<n>	Optional, but support of at least one of the group of options labelled by the same numeral <n> is required
<cid>:	Conditional requirement, according to the condition or item index identified by <cid>
<item>::	Simple predicate condition, dependent on the support marked for <item>

a) Droits de reproduction du formulaire PICS.

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.

A.2 Implementation identification

See Table A.1.

Table A.1 – TLSP Implementation Identification

Item	Information
Supplier	
Contact point for queries about this PICS	
Implementation Name(s) and Version(s)	
Other information necessary for full identification [e.g. Names and Version(s) for machines and operating systems, System Name(s)]	
<p>NOTES</p> <p>1 Only the first three items are required for each implementation. Other information may be completed as appropriate in meeting the requirements for full identification.</p> <p>2 The terms “Name” and “Version” should be interpreted appropriately to correspond with a supplier’s terminology (e.g. using Type, Series, Model).</p>	

A.3 General statement of conformance

Table A.2 codifies the general statement of conformance for the implementation.

Table A.2 – General Conformance Statement

Index Item		Support	
		Y	N
SP	Does the implementation claim conformance with ISO/IEC 10736?	Y	N
SPMAN	Are all mandatory features of ISO/IEC 10736 implemented?	Y	N

A.4 Protocol implementation

Table A.3 identifies common abbreviations used in this PICS, these same abbreviations are found in ITU-T Rec. X.224 | ISO/IEC 8073, but are identified here for help in conforming to this PICS.

Table A.3 – CO and CL Transport Implemented

Index Transport Class Network Service	
C0	Class 0 over cons
C1	Class 1 over cons
C2	Class 2 over cons
C3	Class 3 over cons
C4	Class 4 over cons
C4L	Class 4 over clns
CLTP	Connectionless transport protocol

A.5 Security services supported

Tables A.4 to A.7 identify for each Class of Transport (COTP::), the security services available through the TLSP and their level of support within the implementation. The security services listed are taken from CCITT Rec. X.800 | ISO 7498-2.

Table A.4 – Service Element Proforma for C0

Index Service Element	Status	Support	
TOSE0 Confidentiality	o.1	Y	N
TOSE1 Connection Confidentiality	TOSE0:m	Y	N
TOSE2 Connectionless Confidentiality	–		
TOSE3 Integrity	o.1	Y	N
TOSE4 Connection Integrity w Recovery	–		
TOSE5 Connection Integrity wo Recovery		Y	N
TOSE6 Connectionless Integrity	TOSE3:m		
TOSE7 Peer Entity Authentication	o	Y	N
TOSE8 Access Control	o	Y	N
TOSE9 IN BAND SA-P	o	Y	N

Table A.5 – Service Element Proforma for C1, C2, C3

Index Service Element	Status	Support	
T3SE0 Confidentiality	o.1	Y	N
T3SE1 Connection Confidentiality	T3SE0:m	Y	N
T3SE2 Connectionless Confidentiality	–		
T3SE3 Integrity	o.1	Y	N
T3SE4 Connection Integrity w Recovery	–		
T3SE5 Connection Integrity wo Recovery	T3SE3:o.2	Y	N
T3SE6 Connectionless Integrity	T3SE3:o.2	Y	N
T3SE7 Peer Entity Authentication	o	Y	N
T3SE8 Access Control	o	Y	N

Table A.6 – Service Element Proforma for C4

Index Service Element	Status	Support	
T4SE0 Confidentiality	o.1	Y	N
T4SE1 Connection Confidentiality	T4SE0:m	Y	N
T4SE2 Connectionless Confidentiality	–		
T4SE3 Integrity	o.1	Y	N
T4SE4 Connection Integrity w Recovery	T4SE3:o.2	Y	N
T4SE5 Connection Integrity wo Recovery	–		
T4SE6 Connectionless Integrity	T4SE3:o.2	Y	N
T4SE7 Peer Entity Authentication	o	Y	N
T4SE8 Access Control	o	Y	N

Table A.7 – Service Element Proforma for C4L

Index Service Element	Status	Support	
		Y	N
TLSE0 Confidentiality	o.1	Y	N
TLSE2 Connectionless Confidentiality	TLSE0:m	Y	N
TLSE1 Connection Confidentiality	–		
TLSE3 Integrity	o.1	Y	N
TLSE4 Connection Integrity w Recovery	TLSE3:o.2		
TLSE5 Connection Integrity wo Recovery	–		
TLSE6 Connectionless Integrity	TLSE3:o.2	Y	N
TLSE7 Peer Entity Authentication	o	Y	N
TLSE8 Access Control	o	Y	N

Table A.8 identifies for connectionless Transport (CLTP::), the security services available through the TLSP and their level of support within the implementation.

Table A.8 – Service Element Proforma for CLTP

Index Service Element	Status	Support	
		Y	N
TCSE0 Confidentiality	o.1	Y	N
TCSE1 Connection Confidentiality	–		
TCSE2 Connectionless Confidentiality	TCSE0:m	Y	N
TCSE3 Integrity	o.1	Y	N
TCSE4 Connection Integrity w Recovery	–		
TCSE5 Connection Integrity wo Recovery	–		
TCSE6 Connectionless Integrity	TCSE3:m	Y	N
TCSE7 Data Origination Authentication	o	Y	N
TCSE8 Access Control	o	Y	N

A.6 Supported functions

Tables A.9 to A.16 identify the mandatory and optional functions implemented for each class of Transport (COTP::) supported.

Table A.9 – Mandatory Functions for C0

Index	Function	Reference (subclause)	Status	Support
T0SF1	Verification of peer address	5.6.2, 6.4	m	Y
T0SF2	Reflection detection	5.6.2, 6.3.2	m	Y
T0SF3	Security encapsulation	5.6	m	Y
T0SF4	Reporting of security events	Notes	m	Y

Table A.10 – Optional Functions for C0

Index	Function	Reference (subclause)	Status	Support	
				Y	N
T0SF5	Data encipherment	6.2	o.1	Y	N
T0SF6	Integrity protection	6.3	o.1	Y	N
T0SF7	Integrity padding	6.3.1.3	o	Y	N
T0SF8	Explicit security labeling	6.5	o	Y	N
T0SF9	Encipherment padding	6.2.2	o	Y	N

Table A.11 – Mandatory Functions for C1

Index	Function	Reference (subclause)	Status	Support	
				Y	
T1SF1	Verification of peer address	5.6.2, 6.4	m	Y	
T1SF2	Reflection detection	5.6.2, 6.3.2	m	Y	
T1SF3	Separation after decapsulation	6.1	m	Y	
T1SF4	Security encapsulation	5.6	m	Y	
T1SF5	Reporting of security events	Notes	m	Y	

Table A.12 – Optional Functions for C1

Index	Function	Reference (subclause)	Status	Support	
				Y	N
T1SF6	Data encipherment	6.2	o.1	Y	N
T1SF7	Integrity protection	6.3	o.1	Y	N
T1SF8	Pre-encapsulation concatenation	6.1	o	Y	N
T1SF9	Integrity padding	6.3.1.3	o	Y	N
T1SF10	Explicit security labeling	6.5	o	Y	N
T1SF11	Encipherment padding	6.2.2	o	Y	N

Table A.13 – Mandatory Functions for C2, C3

Index	Function	Reference (subclause)	Status	Support	
				Y	
T3SF1	Verification of peer address	5.6.2, 6.4	m	Y	
T3SF2	Reflection detection	5.6.2, 6.3.2	m	Y	
T3SF3	Separation after decapsulation	6.1	m	Y	
T3SF4	Secure multiplexing	Implicit	m	Y	
T3SF5	Security encapsulation	5.6	m	Y	
T3SF6	Reporting of security events	Notes	m	Y	

Table A.14 – Optional Functions for C2, C3

Index	Function	Reference (subclause)	Status	Support	
T3SF7	Data encipherment	6.2	o.1	Y	N
T3SF8	Integrity protection	6.3	o.1	Y	N
T3SF9	Integrity sequence number space	6.3.3	o	Y	N
T3SF10	Pre-encapsulation concatenation	6.1	o	Y	N
T3SF11	Integrity padding	6.3.1.3	o	Y	N
T3SF12	Explicit security labeling	6.5	o	Y	N
T3SF13	Encipherment padding	6.2.2	o	Y	N

Table A.15 – Mandatory Functions for C4, C4L

Index	Function	Reference (subclause)	Status	Support	
T4SF1	Verification of peer address	5.6.2, 6.4	m	Y	
T4SF2	Reflection detection	5.6.2, 6.3.2	m	Y	
T4SF3	Separation after decapsulation	6.1	m	Y	
T4SF4	Secure multiplexing	Implicit	m	Y	
T4SF5	Security encapsulation	5.6	m	Y	
T4SF6	Reporting of security events	Notes	m	Y	

Table A.16 – Optional Functions for C4, C4L

Index	Function	Reference (subclause)	Status	Support	
T4SF7	Data encipherment	6.2	o.1	Y	N
T4SF8	Integrity protection	6.3	o.1	Y	N
T4SF9	Integrity sequence number	6.3.3	o	Y	N
T4SF10	Pre-encapsulation concatenation	6.1	o	Y	N
T4SF11	Integrity padding	6.3.1.3	o	Y	N
T4SF12	Explicit security labeling	6.5	o	Y	N
T4SF13	Encipherment padding	6.2.2	o	Y	N

Tables A.17 and A.18 identify the mandatory and optional functions implemented for connectionless Transport (CLTP::).

Table A.17 – Mandatory Functions for CLTP

Index	Function	Reference (subclause)	Status	Support	
TLF1	Verification of peer address	5.6.2, 6.4	m	Y	
TLF2	Reflection detection	5.6.2, 6.3.2	m	Y	
TLF3	Security encapsulation	5.6	m	Y	
TLF4	Reporting of security events	5.2.1, 6	m	Y	

Table A.18 – Optional Functions for CLTP

Index	Function	Reference (subclause)	Status	Support	
TLF5	Data encipherment	6.2	o.1	Y	N
TLF6	Integrity protection	6.3	o.1	Y	N
TLF7	Integrity padding	6.3.1.3	o	Y	N
TLF8	Explicit security labeling	6.5	o	Y	N
TLF9	Encipherment padding	6.2.2	o	Y	N

A.7 Supported Protocol Data Units (PDUs)

A.7.1 Supported Transport PDUs (TPDUs)

As indicated in Table A.19 the SE TPDU is supported for both transmission and receipt, for both the connection oriented (COTP::) and connectionless Transport Protocol (CLTP::).

Table A.19 – TPDUs Supported

Index	TPDU	Item	Status	Support	
STS1	SE	Transmission COTP or CLTP	m	Y	
STS2	SE	Receipt COTP or CLTP	m	Y	

A.7.2 Supported parameters of issued TPDUs

Tables A.20 and A.21 indicate which parameters are mandatory or optional when a SE TPDU is issued by Transport (COTP:: or CLTP::).

Table A.20 – Mandatory Parameters for COTP, CLTP

Index	Parameter	Reference (subclause)	Status	Support	
SPI1	Key Identifier must be present.	6.2, 6.3	m	Y	
SPI2	Bit one of Protected Header Flag must be set as direction indicator.	8.2.3.3	m	Y	

Table A.21 – Optional Parameters for COTP, CLTP

Index	Parameter	Reference (subclause)	Status	Support	
SPI3	Label	8.2.3.4	o	Y	N
SPI4	Integrity Pad	8.2.3.6	o	Y	N
SPI5	ICV	8.2.4	o	Y	N
SPI6	Encipherment Pad	8.2.5	o	Y	N

A.7.3 Supported parameters of received TPDUs

Implementations shall be capable of receiving and processing all possible parameters of the SE TPDU as indicated in Table A.22.

Table A.22 – Mandatory parameters for COTP, CLTP

Index	Parameter	Reference (subclause)	Status	Support	
				Y	
SPR1	Key Identifier must be present.	6.2, 6.3	m	Y	
SPR2	Bit one of Protected Header Flag	8.2.3.3	m	Y	
SPR3	Label	8.2.3.4	m	Y	
SPR4	Integrity Pad	8.2.3.6	m	Y	
SPR5	ICV	8.2.4	m	Y	
SPR6	Encipherment Pad	8.2.5	m	Y	

Allowed values of issued TPDU parameters are given in Table A.23.

Table A.23 – Values for Parameters of issued TPDU's for COTP, CLTP

Index	Parameter	Values	
		Allowed	Supported
AVI1	SA-ID	2-126 octets	
AVI2	Prot Header Flags	0 or 1	
	Label		
AVI3	Defining Authority	1-n octets	
AVI4	Value	1-m octets	
	ICV Padding		
AVI5	Length	1-254	
AVI6	Value	1-254 octets	
AVI7		ICV 1-indef octets	
	ENC PADDING		
AVI8	Length	1-254	
AVI9	Value	1-254 octets	

A.7.4 Allowed values of issued TPDU parameters

See Table A.24.

Table A.24 – Values for parameters of received TPDU's for COTP, CLTP

Index	Parameter	Values	
		Allowed	Supported
AVR1	SA-ID	2-126 octets	
AVR2	Prot Header Flags	0 or 1	
	Label		
AVR3	Defining Authority	1-n octets	
AVR4	Value	1-m octets	
	ICV Padding		
AVR5	Length	1-254	
AVR6	Value	1-254 octets	
AVR7	ICV	1-indef octets	
	ENC PADDING		
AVR8	Length	1-254	
AVR9	Value	1-254 octets	

A.8 Service, function, and protocol relationships

A.8.1 Relationship between services and functions

Table A.25 gives a mapping between OSI security services provided by TLSP and the associated functions needed in an implementation. The consistency between supported functions and security services shall be maintained accordingly.

Table A.25 – Mapping of security services to supported functions

Security Service	Functions
Confidentiality	Data encipherment padding
Connection Integrity	Integrity sequence number space Integrity protection Reflection detection padding
Connectionless Integrity	Integrity protection Reflection detection padding
Peer Entity or	Verification of peer address
Data Orig. Authentication	Security encapsulation Use of either: integrity protection or data encipherment
Access Control	Explicit security labeling Secure multiplexing Security encapsulation

A.8.2 Relationship between services and protocol

Table A.26 gives a mapping between OSI security services provided by TLSP and the SE TPDU protocol control information (PCI) and parameter fields employed by the underlying security mechanisms. The consistency between supported security parameters and SE TPDU parameter fields shall be maintained accordingly.

Table A.26 – Mapping of security services to SE TPDU parameters

Security Service	TPDU Parameters/PCI
Confidentiality	Encrypted data Confidentiality padding
Connectionless Integrity	Integrity check value Direction indicator Integrity padding
Connection Integrity	Integrity check value Direction indicator Integrity padding DT/ED send sequence number (final sequence number)
Data Orig. Authentication	Peer address
Peer Entity Authentication	Key identifier Key identifier employed in: integrity check value or encrypted data
Access Control	Security labels Key identifier Key identifier employed in: integrity check value or encrypted data

A.9 Supported algorithms

Table A.27 identifies the set of confidentiality and integrity algorithms supported by this implementation.

Table A.27 – Supported algorithms

Index	Item	Reference (subclause)	Algorithm Identifier ^{a)}
ALG1	Data Encryption	6.2.3	
ALG2	Cryptographic ICV	6.3.1.3	
ALG3	Non-Cryptographic ICV	6.3.1.3	
^{a)} Algorithms supported (if appropriate) under the registration scheme defined in ISO/IEC 9979 or ISO/IEC 9834.			

A.10 Error handling

A.10.1 Security errors

Table A.28 contains the mandatory security error actions to be taken upon receipt of an SE TPDU corresponding to the event description.

A.10.2 Protocol errors

Table A.29 identifies the protocol error actions to be taken upon receipt of an SE TPDU corresponding to the event description.

A.11 Security Association

A.11.1 SA Generic Fields

See Table A.30.

Table A.28 – Mandatory security error actions for COTP, CLTP

Index	Event	Reference (subclause)
SEA1	An improperly protected TPDU received shall be discarded.	6.0
SEA2	A TPDU with an invalid value in the SA-ID identified shall be discarded.	6.2.3
SEA3	A TPDU with an invalid ICV shall be discarded.	6.3.1.3
SEA4	A TPDU with an invalid direction indicator shall be discarded.	6.3.2.3
SEA5	A TPDU with an improper label shall be discarded.	6.5.3
SEA6	A TPDU with an improper Integrity Pad shall be discarded.	6.3.1.3
SEA7	A TPDU with a duplicate sequence number shall be discarded.	6.3.3.3
SEA8	A TPDU with an invalid peer address shall be discarded.	6.4
SEA9	A TPDU with an improper Encipherment Pad shall be discarded.	6.2.2
<p>NOTES</p> <p>1 In item SEA1, an improperly protected TPDU includes both those SE TPDU's where non-negotiated options are used, and those where negotiated options are not used.</p> <p>2 Item SEA7 apply only to the connection oriented Transport Protocol (COTP::) when integrity sequence number space and truncation protection have been negotiated for C2-C4, C4L.</p>		

Table A.29 – Protocol error actions for COTP, CLTP

Index	Event	Reference (subclause)	Action	
			Allowed	Supported
PEA1	An undefined parameter encountered in the protected contents.	8.2.3		
PEA2	Out of sequence parameters discovered in the protected contents.	8.2.3		

Table A.30

Item	Questions/Features	Reference (subclause)	Status	Support on transmission	Support on receipt
SaLI	Length Indicator field transmitted in each SA PDU?	8.3.1	SA:M	Yes N/A	Yes N/A
SaPDUType	PDU Type field with value 01001001 in each SA PDU	8.3.2	SA:M	Yes N/A	Yes N/A
SaSAID	SA-ID field	8.3.3	SA:M	Yes N/A	Yes N/A
SA-PType	SA-P TYPE field	8.3.4	SA:M	Yes N/A	Yes N/A
SA-RK	Is the SA REKEY Supported?	B.5.3	SA:O	Yes No N/A	Yes No N/A
SSLYR*	Is the example SA protocol using Key Token Exchange supported?	Annex B	SA:O	Yes No N/A	Yes No N/A

A.11.2 Content Fields Specific to Key Exchange SA-P

See Table A.31.

Table A.31

Item	Questions/Features	Reference (subclause)	Status	Support on Transmission	Support on receipt
SAExchId	ExchangeID	B.6.1	SAKTE:M	Yes N/A	Yes N/A
ContLen	Is the Length Indicator field transmitted in each SA PDU?	B.6.2	SAKTE:M	Yes N/A	Yes N/A
MySAID	My SAID Content field	B.6.3.1	SAKTE:M	Yes N/A	Yes N/A
OldYrSAID	Old Your SAID Content field	B.6.3.2	SAKTE:M	Yes N/A	Yes N/A
KeyTokens	Key Token 1 and Key Token 2 Content Fields	B.6.3.3	SAKTE:M	Yes N/A	Yes N/A
AuthFields	Authentication digital signature and Authentication certificate Content fields	B.6.3.4	SAKTE:M	Yes N/A	Yes N/A
ServSel	Service Selection Content field	B.6.3.5	SAKTE:O	Yes No N/A	Yes No N/A
SARejReas	SA Rejection Reason Content field	B.6.3.6	SAKTE:O	Yes No N/A	Yes No N/A
SAAbReas	SA Abort/Release Reason Content field	B.6.3.7	SAKTE:M	Yes No N/A	Yes No N/A
LabDef	Label Definition Content field	B.6.3.8	SAKTE:O	Yes No N/A	Yes No N/A
KeySel	Key Selection Content field	B.6.3.9	SAKTE:O	Yes No N/A	Yes No N/A
KeyUse	Usage Flags sub-field	B.6.3.9.	KeySel:M	Yes No N/A	Yes No N/A
KeySelInfo	Key Selection Information sub-field	B.6.3.9.	KeySel:M	Yes No N/A	Yes No N/A
KeyRefx	Key Reference sub-field	B.6.3.9.	KeySel:O	Yes No N/A	Yes No N/A
SaFlags	SA Flags Content field	B.6.3.10	SAKTE:O	Yes No N/A	Yes No N/A
ASSR	ASSR Content field	B.6.3.11	ServSel:M	Yes No N/A	Yes No N/A

Annexe B

Protocole d'association de sécurité utilisant des mécanismes d'échange de jetons de clé et de signatures numériques

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

B.1 Vue d'ensemble

La présente annexe définit un protocole de mise en œuvre d'un mécanisme asymétrique pour l'établissement, le maintien et l'abandon/la libération d'une association SA. Il permet aux entités TLSP communicantes:

- a) de s'authentifier mutuellement;
- b) d'initialiser les attributs SA, y compris les clés; et
- c) d'établir des informations initiales pour assurer l'intégrité.

La présente annexe décrit un protocole SA qui accomplit logiquement les fonctions distinctes suivantes:

- a) un échange de jetons de clé (KTE) (*key token exchange*) est utilisé pour établir un secret partagé. La forme de ces jetons est spécifique du mécanisme adopté. Un exemple de jetons de clé spécifiques du mécanisme adopté et permettant l'échange de clés exponentielles, également appelé échange de Diffie Hellman, est décrit dans l'Annexe C;
- b) des certificats, des signatures numériques et des éléments résultant de l'échange KTE sont utilisés pour assurer l'authentification;
- c) des échanges de données de protocole sont utilisés pour négocier les attributs SA;
- d) des échanges de données de protocole sont utilisés pour signaler que l'association SA est libérée.

Avant d'établir une association SA à l'aide de ce protocole SA, chaque entité TLSP doit avoir préétabli les informations suivantes:

- a) les mécanismes qu'elle met en œuvre, exprimés par:
 - 1) une liste des ensembles de règles ASSR pris en charge; et
 - 2) l'ensemble des services de sécurité assurés pour chacun des ensembles ASSR indiqués ci-dessus;
- b) pour chaque algorithme asymétrique mis en œuvre, une paire de clés asymétriques qui peut être utilisée par l'entité TLSP pour signer des données à des fins d'authentification;
- c) pour chaque algorithme asymétrique mis en œuvre, un certificat d'une autorité de confiance qui identifie l'entité TLSP et sa clé asymétrique publique à des fins d'authentification;
- d) les clés publiques et les algorithmes asymétriques implicites de toute autorité de certification de confiance amenée à délivrer des certificats aux entités TLSP avec lesquelles cette entité TLSP communiquera.

Ce protocole SA établit dynamiquement les informations de sécurité suivantes dont il a besoin pour assurer la sécurité de ses propres communications:

- a) négociation de l'algorithme de codage pour protéger les communications du protocole SA;
- b) négociation de l'algorithme asymétrique et du système de signatures numériques utilisés pour assurer l'authentification du protocole SA;
- c) génération d'informations de codage nécessaires à l'algorithme de codage pour protéger les communications du protocole SA.

Ce protocole SA établit les informations suivantes partagées entre deux entités TLSP:

- a) identificateurs SA-ID local et distant;
- b) services de sécurité qui doivent être utilisés entre les entités associées pour les instances de communication;
- c) mécanismes et leurs paramètres résultant implicitement des services de sécurité sélectionnés;

- d) clés initiales partagées pour les mécanismes d'intégrité et de codage ainsi que pour l'authentification d'une instance de communication;
- e) ensemble d'étiquettes de sécurité qui peuvent être utilisées au titre de cette association pour le contrôle d'accès.

Une association SA peut être établie à l'aide de services de sécurité, de mécanismes avec leurs paramètres et d'un ensemble d'étiquettes de sécurité sélectionnés identiques à ceux d'une association SA précédemment établie. Dans ce cas, seuls l'identificateur SA-ID et les clés sont modifiés, tous les autres attributs restant inchangés.

Chaque fois qu'une nouvelle association SA est établie, de nouvelles valeurs de clé doivent être définies.

Dans le cas du protocole TLSP en mode sans connexion, l'identificateur SA-ID ne doit pas être réutilisé après la libération d'une association SA. La période pendant laquelle un identificateur SA-ID est bloqué doit être supérieure à la durée maximale d'une PDU dans le réseau de base.

L'attribut SA Adr_Served est établi par des moyens qui sortent du cadre de ce protocole.

L'attribut SA entité initiatrice est réglé à la valeur vrai pour l'entité initiatrice de l'échange de données de protocole SA et à la valeur faux pour l'entité répondant à l'appel.

Les échanges de données de protocole pour l'établissement d'une association SA sont illustrés dans la Figure D.1.

B.2 Echange de jetons de clé (KTE)

Les entités TLSP commencent à mettre en œuvre leur protocole SA par un échange de jetons de clé (KTE) pour établir entre elles un secret partagé (c'est-à-dire, une chaîne binaire). Elles utilisent ensuite un sous-ensemble de cette chaîne binaire secrète conjointement avec un algorithme de clé privée pour coder le reste des communications entre elles, assurant ainsi la confidentialité des autres échanges de données de protocole SA.

Le mécanisme KTE consiste à échanger deux valeurs Key Token 1 (jeton de clé n° 1) et Key Token 2 (jeton de clé n° 2) calculées à partir de paramètres spécifiques des mécanismes ainsi que de nombres établis localement à l'aide d'algorithmes spécifiques des mécanismes tels que ceux indiqués dans l'Annexe D. Les valeurs échangées sont utilisées ensuite par les entités communicantes pour créer la chaîne binaire secrète partagée.

Un sous-ensemble de cette chaîne binaire est utilisé conjointement avec un algorithme de clé privée pour coder le reste de l'échange de données de protocole SA assurant l'authentification du protocole SA et la négociation d'attributs SA. En outre, un sous-ensemble de cette chaîne binaire est également référencé pour utilisation sous forme d'attributs de clé et de numéro ISN de l'association de sécurité en cours d'établissement. Ce sous-ensemble est référencé:

- 1) par l'échange d'informations de position lors de la négociation d'attributs SA; ou
- 2) par une connaissance *a priori*.

B.3 Authentification de protocole SA

Pour qu'une entité TLSP puisse en authentifier une autre lors de l'établissement d'une association SA, il faut qu'elle ait un certificat d'authentification et une paire de clés publiques.

Les entités TLSP échangent des certificats et des signatures numériques (tels que ceux définis dans ISO 9594-8) pour vérifier mutuellement leur identité. Un certificat contient, au minimum, certaines informations d'identification d'une entité TLSPE et la clé publique de cette entité (voir la Figure D.1).

Le certificat est certifié par une autorité de confiance et fourni au protocole TLSP à l'aide d'une procédure qui sort du cadre du protocole TLSP. Le certificat porte la signature d'authentification de l'autorité de confiance. Une entité TLSP qui participe à la mise en œuvre de ce protocole SA doit avoir la clé publique de l'autorité de confiance qui a établi le certificat. La méthode utilisée pour obtenir la clé publique de l'autorité de confiance sort du cadre de la présente Norme. Pour qu'une entité TLSP puisse démontrer qu'elle possède un certificat particulier, elle doit prouver qu'elle connaît la clé secrète correspondant à la clé publique dans le certificat.

La preuve de l'actualité des données et de la prévention des attaques visant à répéter les messages dans un but malveillant est apportée par les données signées constituées de nombres déterminés conjointement et spécifiques de la mise en œuvre de ce protocole. A cet effet, les deux entités communicantes A (entité initiatrice de l'association SA) et B (entité répondant à A) procèdent comme suit:

- a) Pour l'entité A, le contenu SA est créé, y compris les champs codés sous forme de TLV qui acheminent:
 - le certificat de l'entité A;
 - les données concernant la négociation des attributs SA (voir B.4) ou les raisons de l'abandon/la libération (voir B.6);

jeton de clé n° 3 calculé en utilisant un algorithme tel que décrit dans l'Annexe D;

sauf l'identificateur ID de l'échange et la longueur de contenu, puis il est signé (par exemple, à l'aide de la signature d'authentification définie dans ISO 9594-8). Le contenu SA, y compris la signature, codée sous forme de TLV, et la longueur de contenu sont alors codés. La clé de codage est constituée des n premiers bits de la chaîne binaire produite par l'échange KTE, n étant le nombre de bits requis par l'algorithme utilisé.

- b) Pour l'entité B, le contenu SA est ensuite créé, signé et codé à l'aide d'informations équivalentes relatives à B et au jeton de clé n° 4 au lieu du jeton de clé n° 3.

Chaque entité vérifie la signature d'authentification de l'entité homologuée en déchiffrant l'échange reçu puis en vérifiant la signature et en contrôlant le jeton de clé pour se protéger des attaques à répétition.

B.4 Négociation d'attributs SA

B.4.1 Négociation des services

En fonction de sa politique de sécurité locale, l'entité TLSP initiatrice établit une ou plusieurs sélections de services de sécurité acceptables. Chaque élément de cet ensemble comprend:

- a) l'attribut ASSR_ID, qui définit la sémantique des services de sécurité sélectionnés (énumérés ci-dessous), pour cet élément; et
- b) une valeur de sélection de service (sémantique définie par l'attribut ASSR_ID) pour chacun des services suivants: confidentialité, authentification, contrôle d'accès, intégrité, et confidentialité du flux de trafic.

En fonction de sa politique de sécurité locale, l'entité TLSP destinataire renverra les informations PCI suivantes à l'entité expéditrice:

- a) si l'un des services de l'ensemble proposé est acceptable, l'entité destinataire renverra un seul élément de service sélectionné;
- b) si aucun des services de l'ensemble proposé n'est acceptable, l'entité destinataire rejettera l'association SA en renvoyant un état indiquant la raison du rejet de l'association SA.

NOTE – La négociation permet à l'une et l'autre des entités TLSP de sélectionner des services de sécurité conformes à sa politique de sécurité locale.

B.4.2 Négociation de l'ensemble d'étiquettes

En fonction de sa politique de sécurité locale, l'entité TLSP initiatrice établit un ensemble d'étiquettes et de références de sécurité dont elle accepte le transfert dans le cadre de la protection de cette association SA. Chaque élément de cet ensemble contient la sémantique complète de l'étiquette.

En fonction de sa politique de sécurité locale, l'entité TLSP destinataire détermine laquelle des étiquettes de l'ensemble proposé elle accepte de transférer dans le cadre de la protection de cette association SA. L'entité TLSP destinataire renverra les informations PCI suivantes à l'entité expéditrice:

- a) si une ou plusieurs étiquettes de l'ensemble proposé sont acceptables, l'entité destinataire renverra un sous-ensemble de l'ensemble de références proposé. Les ensembles nuls ne sont pas autorisés;
- b) si aucune des étiquettes de l'ensemble proposé n'est acceptable, l'entité destinataire rejettera l'association SA en renvoyant un état indiquant la raison du rejet de l'association SA.

NOTE – Cette négociation permet à l'une et l'autre des entités TLSP de sélectionner un ensemble d'étiquettes conforme à sa politique de sécurité locale. Les opérations indiquées ci-dessus ne sont applicables que si l'attribut label a été sélectionné.

B.4.3 Sélection de clés et de numéros ISN

En fonction de sa politique de sécurité locale, l'entité TLSP initiatrice sélectionne les parties de la chaîne binaire qui résultent de l'échange KTE pour les utiliser comme clés et/ou numéros ISN pendant les communications (c'est-à-dire, les communications TLSP et non les communications de protocole SA) avec l'entité TLSP destinataire. La clé ou le numéro ISN sont identifiés par la communication de la position du bit de départ dans la chaîne binaire résultant de l'échange KTE. La longueur de la clé/du numéro ISN est déterminée à partir des paramètres associés au service sélectionné. Un ensemble de pointeurs est envoyé à l'entité TLSP destinataire pour les informations suivantes:

- a) clé de codage de données normales;
- b) clé de codage de données exprès;

- c) clé de génération de contrôle d'intégrité de données normales;
- d) clé de génération de contrôle d'intégrité de données exprès;
- e) attribut My ISN pour données normales;
- f) attribut My ISN pour données exprès; et
- g) clé de génération d'authentification.

De même, l'entité TLSP destinataire détermine, en fonction de sa politique de sécurité locale, les parties de la chaîne binaire résultant de l'échange KTE qu'elle utilisera comme clés/numéros ISN. L'entité TLSP destinataire renverra les informations PCI suivantes à l'entité expéditrice:

- a) si l'entité destinataire décide d'utiliser les mêmes positions de bit que celles proposées par l'entité TLSP initiatrice, aucune information PCI explicite n'est renvoyée;
- b) si l'entité destinataire rejette l'association SA en raison d'autres échecs de négociation, aucune information PCI explicite n'est renvoyée;
- c) si l'entité destinataire sélectionne des positions de bit différentes pour ses clés/numéros ISN, elle renverra un ensemble de pointeurs.

NOTE – La même valeur de clé peut être utilisée à des fins multiples, auquel cas le même pointeur est envoyé pour plusieurs clés/numéros ISN.

B.4.4 Négociation de divers attributs SA

En fonction de sa politique de sécurité locale, l'entité TLSP initiatrice détermine la valeur des autres attributs SA sélectionnés pour l'association SA en cours d'établissement, par exemple, «retain these SA attributes on disconnect» (maintien de ces attributs SA lors de la déconnexion) (Rec. UIT-T X.224 | ISO/CEI 8073).

L'entité TLSP initiatrice envoie à l'entité TLSP destinataire cet ensemble d'attributs SA proposés dans un champ marqueurs divers.

En fonction de sa politique de sécurité locale, l'entité TLSP destinataire renvoie les informations PCI suivantes à l'entité expéditrice:

- a) si l'entité destinataire accepte tous les attributs SA proposés, aucune information PCI explicite n'est renvoyée. Si l'entité destinataire ne rejette pas l'association SA, cela implique que les attributs SA sont acceptables pour cette entité;
- b) si aucun des attributs n'est acceptable, l'entité destinataire rejette l'association SA en renvoyant un état indiquant quels attributs ont été la cause du rejet.

B.4.5 Vue d'ensemble de la modification de clés

Si une association SA est établie pour modifier les clés d'une ancienne association SA, seule la sélection de clés et de numéros ISN est effectuée. Au lieu de la négociation des services, de l'ensemble d'étiquettes et des divers attributs SA, une référence à l'ancienne association SA dont ces attributs doivent être hérités, est placée dans l'attribut Old_Your_SA-ID.

B.4.6 Vue d'ensemble de la procédure d'abandon/de libération d'une association SA

Une association de sécurité peut être libérée à l'aide des méthodes suivantes:

- a) par l'échange d'unités de données de protocole d'association de sécurité;
- b) par l'utilisation de mécanismes externes qui sortent du cadre du protocole de couche inférieure;
- c) implicitement par la fermeture d'une connexion;
- d) implicitement lorsqu'une clé de l'association SA expire.

Ces méthodes de libération d'une association SA se divisent en deux catégories, à savoir la méthode hors bande et la méthode dans la bande. Dans le cas de la méthode dans la bande, il est possible de libérer l'association SA par une demande de déconnexion de la connexion de transport ou par l'émission d'une SA PDU avec un type de champ de contenu raison de l'abandon/la libération SA. Voir B.6.3 pour de plus amples détails.

B.5 Mise en correspondance des fonctions de protocole SA avec les échanges de données de protocole

Ce protocole SA assure les trois fonctions indiquées au début de la présente annexe lors de trois échanges distincts de données de protocole:

- a) le premier consiste en un échange de jetons de clé (KTE) et de certificats; il ne fait pas l'objet d'un codage;
- b) le deuxième consiste en une négociation de la sécurité protégée pour assurer l'authentification comme indiqué au B.3;
- c) un échange distinct déclenché lorsque l'association SA n'est plus nécessaire porte sur un code de raison protégé pour assurer l'authentification comme indiqué au B.3.

B.5.1 (Premier) Echange de jetons de clé (KTE)

B.5.1.1 Demande d'initialisation d'un protocole SA

L'entité TLSP ou le système local de gestion de la sécurité initialise le protocole SA.

L'entité TLSP initiatrice assure les fonctions suivantes et envoie les informations suivantes à l'entité destinataire:

- a) un identificateur SA-ID disponible est sélectionné et placé comme attribut My_SA-ID de l'entité expéditrice;
- b) un échange KTE est déclenché et la valeur «Key Token 1» est envoyée;
- c) une liste de mécanismes de confidentialité qu'il est proposé d'utiliser pour protéger le deuxième échange de données de protocole SA est envoyée. Cette liste est exprimée sous la forme d'un ou de plusieurs éléments qui comprennent l'identificateur ASSR_ID et les services de sécurité «confidentialité» sélectionnés. Il n'est pas nécessaire que cette liste soit envoyée si des mécanismes ont été préalablement convenus;
- d) une liste de mécanismes d'intégrité proposés, dont un serait utilisé pour signer numériquement le deuxième échange de données de protocole SA est envoyée. Cette liste est exprimée sous la forme d'un ou de plusieurs éléments qui comprennent l'identificateur ASSR_ID et les services de sécurité «intégrité» sélectionnés. Il n'est pas nécessaire que cette liste soit envoyée si des mécanismes ont été préalablement convenus.

NOTE – Les services de sécurité confidentialité sélectionnés doivent seulement identifier un algorithme de codage symétrique et son mode de fonctionnement. Les services de sécurité intégrité sélectionnés doivent seulement identifier un algorithme asymétrique et son système de signature numérique associé. Les points c) et d) peuvent être connus *a priori*.

Dans le cas du mode CO, si aucune PDU n'est renvoyée lors du premier échange après une temporisation, l'association SA n'est pas établie et aucune autre tentative n'est faite.

Dans le cas du mode CL, si aucune PDU n'est renvoyée lors du premier échange après une temporisation, l'entité TLSP initiatrice transmet à nouveau sa PDU du premier échange. Les nouvelles transmissions sont limitées à un nombre fini qui est déterminé localement.

B.5.1.2 Réception de la PDU du premier échange par l'entité destinataire

A la réception de la PDU du premier échange, l'entité TLSP destinataire assure les fonctions suivantes et envoie les informations suivantes à l'entité initiatrice:

- a) l'attribut My_SAID reçu est placé dans le champ Your_SAID de l'en-tête générique comme indiqué au 8.3;
- b) un identificateur SAID disponible est sélectionné et envoyé comme attribut My_SAID d'entité expéditrice;
- c) en fonction de sa politique de sécurité locale, l'entité TLSP destinataire renvoie les informations PCI suivantes à l'entité initiatrice:
 - 1) si l'entité destinataire accepte l'un des mécanismes de confidentialité proposés, elle renvoie le mécanisme sélectionné. Si l'entité initiatrice a proposé un seul mécanisme, aucune information PCI explicite n'est renvoyée;
 - 2) si aucun des mécanismes de confidentialité n'est acceptable, l'entité destinataire rejette l'association SA en renvoyant un état indiquant la cause du rejet;

- d) en fonction de sa politique de sécurité locale, l'entité TLSP destinataire renvoie les informations PCI suivantes à l'entité expéditrice:
 - 1) si l'entité destinataire accepte l'un des mécanismes d'intégrité proposés, elle renvoie le mécanisme sélectionné. Si l'entité initiatrice a proposé un seul mécanisme, aucune information PCI explicite n'est renvoyée;
 - 2) si aucun des mécanismes d'intégrité n'est acceptable, l'entité destinataire rejette l'association SA en renvoyant un état indiquant la cause du rejet;
- e) sous réserve qu'un mécanisme ait été sélectionné aussi bien pour la confidentialité que pour l'intégrité, le calcul relatif à l'échange KTE est déclenché et la valeur Key-Token-2 est envoyée.

Dans le cas du mode CO, si aucune PDU n'est renvoyée lors du deuxième échange après une temporisation, l'association SA n'est pas établie et aucune autre tentative n'est faite.

Dans le cas du mode CL, si aucune PDU n'est renvoyée lors du deuxième échange après une temporisation, l'entité TLSP initiatrice transmet à nouveau sa PDU du premier échange. Les nouvelles transmissions sont limitées à un nombre fini qui est déterminé localement.

Dans le cas du mode CL, si la PDU du premier échange est à nouveau reçue, la PDU de retour est à nouveau envoyée.

B.5.2 (Deuxième) Echange de négociation de l'authentification et de la sécurité

B.5.2.1 Réception de la PDU du premier échange par l'entité initiatrice

A la réception de la PDU du premier échange, l'entité TLSP initiatrice assure les fonctions suivantes et envoie les informations suivantes à l'entité destinataire:

- a) l'attribut My_SAID reçu est placé dans le champ Your_SAID de l'en-tête générique comme indiqué au 8.3;
- b) le certificat de l'entité initiatrice associé au mécanisme d'intégrité sélectionné est placé dans le champ de contenu certificat;
- c) le destinataire établit le jeton de clé n° 3;
- d) une liste de services de sécurité qu'il est proposé d'utiliser pour protéger la communication TLSP est placée dans le champ de contenu sélection de services;
- e) un ensemble d'étiquettes qu'il est proposé d'utiliser pour protéger cette association SA au cours de la communication TLSP est placé dans l'attribut Label_Def;
- f) un ensemble de pointeurs de clés/numéro ISN est placé dans le champ sélection de clés;
- g) les divers attributs SA nécessaires pour cette association SA sont placés dans des marqueurs SA;
- h) si l'association SA est établie pour modifier les clés d'une ancienne association SA, l'attribut Old Your SA-ID est réglé à la valeur de l'identificateur SA-ID de l'ancienne association SA dont les clés doivent être modifiées. Si ce processus est mis en œuvre, les opérations indiquées en d), e) et g) ci-dessus ne doivent pas être effectuées;
- i) le contenu SA est protégé comme indiqué au B.3.

Dans le cas du mode CO, si aucune PDU n'est renvoyée lors du deuxième échange après une temporisation, l'association SA n'est pas établie et aucune autre tentative n'est faite.

Dans le cas du mode CL, si aucune PDU n'est renvoyée lors du deuxième échange après une temporisation, l'entité TLSP initiatrice transmet à nouveau sa PDU du deuxième échange. Les nouvelles transmissions sont limitées à un nombre fini qui est déterminé localement.

Dans le cas du mode CL, si la PDU du premier échange est à nouveau reçue, la PDU du deuxième échange est à nouveau envoyée.

B.5.2.2 Réception de la PDU du deuxième échange par l'entité destinataire

A la réception de la PDU du deuxième échange, l'entité TLSP destinataire assure les fonctions suivantes et envoie les informations suivantes à l'entité initiatrice:

- a) l'attribut My_SAID reçu est placé dans le champ Your_SAID de l'en-tête générique comme indiqué au 8.3;

- b) les points suivants sont vérifiés. Si la vérification d'un point quelconque échoue, l'association SA est rejetée et un champ état indiquant la cause du rejet est renvoyé:
 - 1) la signature numérique reçue est vérifiée pour déterminer si elle est valide;
 - 2) le jeton de clé n° 3 reçu est vérifié pour déterminer s'il est valide;
 - 3) l'ensemble de services de sécurité proposés est vérifié pour déterminer si l'un quelconque de ces services est acceptable. Un seul des services de sécurité proposés peut être sélectionné;
 - 4) l'ensemble des étiquettes proposées est vérifié pour déterminer si l'une quelconque de ces étiquettes est acceptable;
 - 5) les divers attributs SA sont vérifiés pour déterminer s'ils sont tous acceptables;
- c) si l'attribut Old Your-SA-ID est présent dans la PDU reçue, les attributs SA appropriés sont copiés à partir de l'identificateur SA-ID référencé. Dans ce cas, les champs indiqués en c), d) ci-dessous ne peuvent être envoyés.

Sous réserve que toutes les vérifications aient abouti, les fonctions suivantes sont mises en œuvre:

- a) le certificat d'entité initiatrice associé au mécanisme d'intégrité sélectionné est envoyé;
- b) les services de sécurité sélectionnés qui doivent être utilisés pour protéger la communication TLSP sont envoyés. Si l'ensemble des services proposés contenait un seul élément, aucune information PCI n'est renvoyée;
- c) le destinataire établit le jeton de clé n° 4;
- d) le sous-ensemble sélectionné d'étiquettes qu'il est proposé d'utiliser pour protéger cette association SA au cours de la communication TLSP est envoyé;
- e) un ensemble de pointeurs de clé/numéro ISN est envoyé. Si les pointeurs de l'entité initiatrice sont acceptables pour l'entité destinataire, aucune information PCI n'est envoyée;
- f) le contenu SA est protégé comme indiqué au B.3.

Dans le cas du mode CL, si la PDU du deuxième échange est à nouveau reçue, l'entité destinataire envoie à nouveau sa PDU du deuxième échange.

B.5.3 Procédure de modification de clés

Les entités TLSP peuvent, à tout moment au cours d'une association de sécurité, mettre à jour les clés par un échange d'informations SCI. Cet échange est transparent pour l'utilisateur TLSP et aucune primitive de service TLSP n'est définie pour l'invoquer.

L'un des modes de mise en œuvre possibles est l'échange d'informations SCI à intervalles réguliers (par exemple, toutes les heures ou toutes les 10 000 SE TPDU) au cours d'une connexion. La modification des clés entraînera la sélection d'un nouvel identificateur SA-ID; cependant, les attributs peuvent être hérités de l'association SA en vigueur.

Les informations de modification de clés peuvent contenir:

- a) une nouvelle clé codée à l'aide d'une clé de codage de clé (KEK) mutuelle;
- b) une nouvelle clé codée à l'aide de la clé publique du destinataire;
- c) une référence à une clé précédemment répartie;
- d) les informations de modification de clés utilisées par une méthode de répartition de clés précédemment agréée.

Les procédures de modification de clés sont fondées sur l'échange de deux SA PDU contenant des informations de modification de clés (appelées informations aller et informations retour) ainsi que des SE TPDU normales comme suit.

Une SA PDU contenant des informations de modification de clés aller est préparée avec:

- a) marqueur aller/retour réglé à 0 dans l'octet des marqueurs;
- b) attribut Label-Ref réglé à la référence de l'étiquette appropriée, si le mécanisme d'étiquetage est sélectionné;
- c) informations de clé réglées conformément au mécanisme de répartition de clés;
- d) numéro ISN initial protégé réglé au numéro de séquence de la SE TPDU qui doit être codée à l'aide de la clé mise à jour;
- e) marqueur SA modification de clé, champ n° 3, réglé à 1.

A la réception d'une SA PDU contenant des informations de modification de clés aller:

- a) il convient de vérifier que la valeur du champ Label-Ref est valable pour cette association SA si le mécanisme d'étiquetage est sélectionné;
- b) les informations de clé sont traitées conformément au mécanisme de répartition de clés;
- c) il convient de vérifier si le numéro ISN initial est approprié ou non;
- d) il convient de vérifier que le marqueur «modification de clé», champ n° 3, est réglé à 1.

Une SA PDU contenant des informations de modification de clés retour est préparée avec:

- a) marqueur aller/retour réglé à 1 dans l'octet des marqueurs;
- b) attribut Label-Ref réglé à la référence de l'étiquette appropriée si le mécanisme d'étiquetage est sélectionné;
- c) informations de clé réglées conformément au mécanisme de répartition de clés;
- d) numéro ISN initial protégé réglé au numéro de séquence de la SE TPDU qui doit être chiffrée à l'aide de la clé mise à jour;
- e) marqueur SA modification de clé, champ n° 3, réglé à 1.

A la réception d'une SA PDU contenant des informations de modification de clés retour:

- a) il convient de vérifier que la valeur du champ Label-Ref est valable pour cette association SA si le mécanisme d'étiquetage est sélectionné;
- b) les informations de clé sont traitées conformément au mécanisme de répartition de clés;
- c) il convient de vérifier si le numéro ISN initial est approprié ou non;
- d) il convient de vérifier que le marqueur modification de clé, champ n° 3, est réglé à 1.

En cas de vérification positive de la réponse, si l'entité TLSP n'a aucune TPDU en attente d'encapsulation, une SA PDU ne contenant aucune donnée est envoyée pour terminer la procédure de modification de clés.

Lorsqu'une entité TLSP qui a envoyé une SE TPDU contenant des informations de modification de clé aller reçoit une SE TPDU encapsulée à l'aide de la clé précédente, elle ne doit pas la rejeter, sauf en cas de dispositions contraires de la politique de sécurité.

Si la procédure de modification de clés échoue, l'association est réétablie à l'aide du protocole SA-P ou par tout autre moyen approprié.

B.5.4 Echange pour la libération/l'abandon de l'association SA

B.5.4.1 Demande d'initialisation de la libération/de l'abandon de l'association SA

L'entité TLSP ou le système local de gestion de la sécurité initialise la libération/l'abandon de l'association SA. L'entité initiatrice de l'abandon/la libération de l'association SA n'est pas nécessairement l'entité initiatrice de l'établissement de cette association.

- a) Si l'entité locale est l'initiateur d'établissement SA alors le jeton de clé n° 3 est établi, autrement le jeton de clé n° 4 est établi. Dans les deux cas, le jeton établi est placé dans les contenus SA;
- b) le code de raison approprié est placé dans le champ de contenu SA raison de l'abandon/la libération;
- c) le contenu SA est protégé comme indiqué au B.3.

Dans le cas du mode CO si, à la suite de la demande d'abandon/de libération, une PDU de confirmation n'est pas renvoyée après une temporisation, l'association SA n'est pas établie et aucune autre tentative n'est faite.

Dans le cas du mode CL si, à la suite de l'échange relatif à l'abandon/la libération, une PDU n'est pas renvoyée après une temporisation, l'entité TLSP initiatrice transmet à nouveau sa PDU de demande de libération/d'abandon SA. Les nouvelles transmissions sont limitées à un nombre fini qui est déterminé localement.

B.5.4.2 Réception d'une demande d'abandon/de libération SA

A la réception de la PDU de confirmation d'abandon/de libération SA, l'entité TLSP destinataire assure les fonctions suivantes et envoie les informations suivantes à l'entité initiatrice:

- a) si l'entité locale est l'initiateur d'établissement SA alors le jeton de clé n° 3 est établi, autrement le jeton de clé n° 4 est établi. Dans les deux cas, le jeton établi est placé dans les contenus SA;
- b) le code de raison approprié est placé dans le champ de contenu SA raison de l'abandon/de la libération;
- c) le contenu SA est protégé comme indiqué au B.3.

Dans le cas du mode CL, si la PDU de la demande d'abandon/de libération est à nouveau reçue, l'entité destinataire envoie à nouveau sa PDU du deuxième échange, ces nouveaux envois étant limités à un nombre donné.

B.6 SA PDU – Contenu SA

Pour ce protocole SA spécifique, le format du champ de contenu SA de la SA PDU défini au B.4 est indiqué sur la Figure B.2.

ID d'échange	Longueur de contenu	Champ de contenu	Champ de . . . contenu
1	2	var	var

Figure B.2 – Contenu SA

B.6.1 ID d'échange

Ce champ contient une valeur de 00000000 si la PDU est associée au premier échange de jetons de clé et une valeur de 00000001 si la PDU est associée au deuxième échange d'authentification/de négociation. Ce champ contient une valeur de 10000000 si la PDU est associée à une demande d'abandon/de libération SA et une valeur de 10000001 si la PDU est associée à une confirmation d'abandon/de libération SA.

B.6.2 Longueur de contenu

Longueur en octets de tous les champs de contenu à l'exception du champ longueur de contenu.

B.6.3 Champs de contenu

Le codage du type de champ de contenu est défini au 8.2. Les champs de contenu SA (c'est-à-dire, 00-BF) utilisés par les procédures de cette annexe sont indiqués ci-dessous:

<i>Valeur</i>	<i>Type de champ de contenu</i>
A0	My SA-ID
A1	Old Your-SA-ID
A2	Key Token 1
A3	Key Token 2
A4	Signature numérique d'authentification
A5	Certificat d'authentification
A6	Sélection de services
A7	Raison du rejet SA
A8	Raison de l'abandon/la libération SA
A9	Marqueurs SA
AA	Sélection de clés
AB	ASSR
AC	Entité initiatrice
AD	Algorithme d'intégrité
AE	Algorithme de confidentialité
AF	Longueur d'ICV
B1	Clé de codage
B2	Clé de décodage
B3	Mécanisme d'authentification
B4	Mécanisme de contrôle d'accès
B5	Jeton de clé n° 3
B6	Jeton de clé n° 4
B7-BF	Réservé pour utilisation future

NOTE – D'autres codes sont réservés pour utilisation privée au 8.2 du texte principal de la présente Recommandation | Norme internationale.

ISO/CEI 10736-4 : 1995 (F)

Les champs sélection de services, raison du rejet SA, Label-Def, marqueurs SA et sélection de clés sont optionnels dans cette définition spécifique de contenu du protocole SA.

B.6.3.1 My_SA-ID

Ce champ obligatoire n'est utilisé que lors du premier échange. Ce paramètre est l'identificateur local d'une association de sécurité.

B.6.3.2 Old Your-SA-ID

Ce champ est utilisé lors du deuxième échange si les attributs, autres que les clés, doivent être hérités de l'ancienne association SA.

B.6.3.3 Key Token 1 et Key Token 2, Key Token 3 et Key Token 4

Ces champs obligatoires sont utilisés pour la mise en œuvre de l'échange KTE comme indiqué précédemment dans la présente annexe.

B.6.3.4 Signature numérique d'authentification, Certificat

Ces champs obligatoires sont utilisés pour assurer l'authentification comme indiqué précédemment dans la présente annexe.

B.6.3.5 Sélection de services

Ce champ facultatif est utilisé lors des premier et deuxième échanges:

- a) s'il est utilisé lors du premier échange, il sert à identifier les mécanismes de confidentialité et/ou d'intégrité qu'il est proposé d'utiliser lors du deuxième échange de données de protocoles SA. Dans ce cas, seuls les deux premiers octets sont présents;
- b) s'il est utilisé lors du deuxième échange, il sert à proposer tous les mécanismes qui doivent être mis en œuvre pendant les communications TLSP protégées par l'association SA en cours d'établissement.

Ce champ peut être inclus une ou plusieurs fois dans la PDU du premier ou du deuxième échange de manière à former un ensemble de services de sécurité proposé pour la négociation.

Ce paramètre contient une séquence d'octets indiquant les niveaux des services de sécurité sélectionnés. La sémantique des niveaux est définie dans le cadre de la politique de sécurité. Les octets pour chacun des services de sécurité apparaissent dans l'ordre indiqué ci-dessous. La séquence d'octets peut être tronquée si les octets tronqués se rapportent tous aux services qui ont la valeur QOS 0. Un seul octet de valeur 255 indique que les services de sécurité sélectionnés ont été préétablis.

<i>Octet</i>	<i>Signification</i>
1	Confidentialité en mode sans connexion/Confidentialité en mode connexion
2	Intégrité en mode sans connexion/Intégrité en mode connexion avec ou sans reprise
3	Authentification de l'origine des données/Authentification de l'entité homologue
4	Contrôle d'accès
5	Protection du système d'extrémité
6	Protection connexion par connexion

B.6.3.6 Raison du rejet SA

Ce champ facultatif peut être présent dans la PDU du premier ou du deuxième échange. Il est présent pour indiquer le rejet de l'association SA au cours de son établissement. Il contient la raison du rejet comme suit:

<i>Valeur</i>	<i>Signification</i>
1	Mécanisme de confidentialité non pris en charge
2	Mécanisme d'intégrité non pris en charge
3	Mécanisme de contrôle d'accès non pris en charge
4	Mécanisme d'authentification non pris en charge
5	Système d'extrémité non pris en charge
6	Protection connexion par connexion non prise en charge
7	Mécanisme de confidentialité rejeté
8	Mécanisme d'intégrité rejeté
9	Mécanisme de contrôle d'accès rejeté

10	Mécanisme d'authentification rejeté
11	Signature d'authentification non valide
12	Certificat non valide
13	Ensemble d'étiquettes proposé rejeté
14	Attribut Retain_on_Disconnect rejeté
15	Attribut Param_Prot rejeté
16	Système d'extrémité rejeté
17	Protection connexion par connexion rejetée

B.6.3.7 Raison de l'abandon/la libération SA

Ce champ obligatoire est présent dans la demande et l'indication d'abandon/de libération SA. Il est utilisé pour indiquer la raison de l'abandon/la libération d'une association SA.

Il est réglé à 0 pour l'abandon et à 1 pour la libération normale. Les valeurs 2 à 127 sont réservées pour utilisation future. D'autres valeurs peuvent être utilisées pour des codes de raison définis à titre privé.

B.6.3.8 Label

Ce champ facultatif n'est utilisé que dans la PDU de deuxième échange, comme indiqué au 8.2.3.4. L'entité initiatrice proposera un ensemble d'étiquettes de sécurité. Le destinataire peut sélectionner l'ensemble complet ou un sous-ensemble des étiquettes que l'entité initiatrice a envoyées. Si l'ensemble initial n'est pas acceptable, le destinataire peut proposer un ensemble d'étiquettes différent.

B.6.3.9 Sélection de clés

Ce champ facultatif n'est utilisé que dans la PDU du deuxième échange. Il peut apparaître un nombre quelconque de fois dans le contenu SA.

Ce champ est subdivisé en trois sous-champs:

- a) marqueurs d'utilisation;
- b) information de sélection de clés;
- c) référence de clé.

B.6.3.9.1 Marqueurs d'utilisation

Ce champ contient jusqu'à sept valeurs indiquant la position dans la chaîne binaire résultante de l'échange KTE où certaines clés doivent prendre leur valeur. La longueur de la clé est déterminée à partir du service de sécurité associé sélectionné qui identifie l'algorithme associé. Des clés multiples peuvent utiliser la même position de bit (c'est-à-dire la même clé). Les combinaisons admissibles dépendent de la politique de sécurité locale.

<i>Octet</i>	<i>Position de clé/d'ISN correspondante dans la chaîne binaire EKE</i>
1-2	Clé de codage de données normales
3-4	Clé de codage de données exprès
5-6	Clé de génération de contrôle d'intégrité de données normales
7-8	Clé de génération de contrôle d'intégrité de données exprès
9-10	Attribut My ISN pour données normales
11-12	Attribut My ISN pour données exprès
13-14	Clé de génération d'authentification

Si le destinataire désire utiliser les mêmes clés que l'entité appelante, ce champ ne doit pas être présent dans la PDU du deuxième échange du destinataire.

B.6.3.9.2 Informations de sélection de clés

Ce champ indique la position, dans la chaîne binaire résultant de l'échange KTE, où les clés sélectionnées doivent prendre leur valeur. La longueur des clés est déterminée à partir du service de sécurité associé sélectionné qui identifie l'algorithme associé. Des clés multiples peuvent utiliser la même position de clé (c'est-à-dire, la même clé). Les combinaisons admissibles dépendent de la politique de sécurité locale.

B.6.3.9.3 Référence de clé

Ce sous-champ facultatif peut être utilisé pour permettre une référence ultérieure à la clé, par exemple, à des fins d'audit ou pour la sélection d'une nouvelle clé pour une connexion qui utilise la SA PDU. La valeur de cette référence doit être unique pour l'association de sécurité.

B.6.3.10 Marqueurs SA

Les positions de bit indiquées ci-dessous sont utilisées pour signaler les attributs SA identifiés. La valeur 0 a la signification faux. La valeur 1 a la signification vrai.

<i>Bit</i>	<i>Attribut SA</i>
1	Retain-on-Disconnect
2	Param_Protect
3	Modification de clés
4	Informations aller/retour
5-8	Réservé pour utilisation future

Les bits 5 à 8 sont réglés à 0 lors de la transmission et sont ignorés lors de la réception.

B.6.3.11 ASSR

Ce champ doit être présent si le champ sélection de services est présent. C'est l'identificateur d'objet (défini dans ISO/CEI 9834) qui identifie l'ensemble de règles de sécurité définissant les mécanismes à appliquer en fonction du paramètre QOS de protection sélectionné.

Annexe C

Exemple d'ensemble agréé de règles de sécurité (ASSR)

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

Un ensemble agréé de règles de sécurité (ASSR) (*agreed set of security rules*) établit les mécanismes de sécurité à mettre en place pour assurer une qualité de service de protection donnée, y compris tous les paramètres nécessaires pour définir le fonctionnement de ce mécanisme.

ASSR-ID { joint-iso-ccitt (2) identified organization (3) oiw (14) secsig (3) oiwsecsigassrobjectidentifier (5) rule (1) } (Object Identifier)

SA-ID Length 4 Octets

Protection QOS Definition Module

PE Auth:	low
AC:	none
Confid:	high
Integ:	high
Security Label:	none

Protection of all service parameters

For Protection QOS: Integ = high Confid = high

Mechanism Module – Security Labels for Access Control

For Protection QOS: AC = high or Conf = high

Label_Def_Auth XYZ

Explicit indication: Yes

Mechanism Module – Integrity Check Value

For Protection QOS: Integ .none or Auth = High
or Mechanism for Security Labels

ICV_Alg_ID	XYZ
ICV_Block_size	8 octets
Rekey after	15000 PDUs
Key Distribution mech	Asymmetric

Mechanism Module – Integrity Sequence Number

For Protection QOS: Integ = high Auth = high

ISN_Len 4 octets

Mechanism Module – Encipherment

For Protection QOS: Conf > low

Enc_Alg_ID	XYZ
Mode	Chained
Enc_Block_Size	8 octets
Rekey after	10000 PDUs
Key Distribution mech	Asymmetric

Mechanism Module – Connection Authentication

For Protection QOS: AC > low or PE Auth > Low

Enc_Alg_ID XYZ

Mechanism Module – Asymmetric Key Distribution

For mechanism encipherment or Integrity check value

PKC_Alg_ID RSA

Mechanism Module – Symmetric Key Distribution

For mechanism encipherment or Integrity check value

PKC_Alg_ID DES (X9.17)

Annexe D

Vue d'ensemble de l'algorithme EKE

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

Deux paramètres sont nécessaires pour l'échange EKE. L'un est un nombre premier p élevé (tel que $p-1$ ait un facteur premier élevé), l'autre un nombre « a » inclus dans les limites 1, a , $p-1$.

Soit A et B les deux entités communicantes (voir la Figure D.1). L'échange EKE débute par le choix, par A, d'un nombre aléatoire X élevé et par le choix, par B, d'un nombre aléatoire Y élevé. A calcule alors la formule $(a^{**X} \bmod p)$ et envoie a , p et $(a^{**X} \bmod p)$ à B qui calcule la formule $(a^{**XY} \bmod p)$ et l'envoie à A. A et B calculent la formule $(a^{**XY} \bmod p)$. Seules les formules $(a^{**X} \bmod p)$ et $(a^{**Y} \bmod p)$ sont visibles pour un observateur étranger. Il est impossible à cet observateur de déterminer X ou Y , donc de calculer la formule $(a^{**XY} \bmod p)$.

A et B peuvent utiliser ultérieurement, comme clés, des sous-ensembles des éléments binaires contenus dans la formule $(a^{**XY} \bmod p)$.

Les valeurs décrites dans le protocole SA défini dans l'Annexe B sont les suivantes:

- la chaîne binaire EKE partagée est égale à $(a^{**XY} \bmod p)$;
- la valeur du jeton Key Token 1 est égale à a , p , $(a^{**X} \bmod p)$ où 'a', 'p' et $(a^{**X} \bmod p)$ sont codés sous la forme d'une chaîne d'octets;
- la valeur du jeton Key Token 2 est égale à $(a^{**Y} \bmod p)$;
- le jeton de clé n° 3 est l'information dérivée de la chaîne de bit KTE partagée $(a^{**XY} \bmod p)$ pour contrer les attaques à répétition;
- le jeton de clé n° 4 est l'information dérivée de la chaîne de bit KTE partagée $(a^{**XY} \bmod p)$ pour contrer les attaques à répétition.

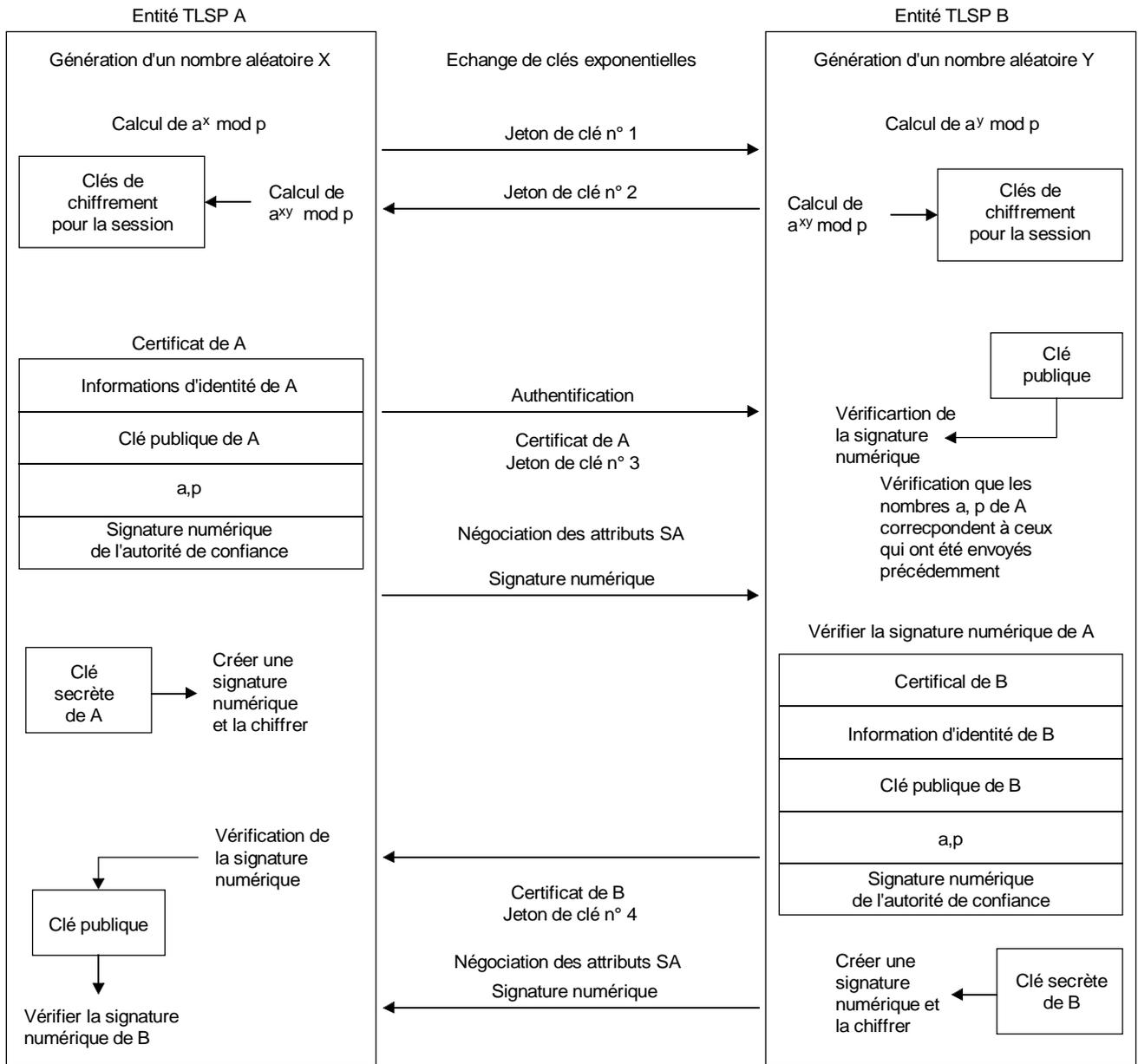


Figure D.1 – Illustration du mécanisme de calcul de clés et d'échange de signatures numériques utilisant l'algorithme EKE en cours de communication