UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T X.273

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 – INTERCONNEXION DES SYSTÈMES OUVERTS – PROTOCOLE DE SÉCURITÉ DE LA COUCHE RÉSEAU

Recommandation UIT-T X.273

(Antérieurement «Recommandation du CCITT»)

AVANT-PROPOS

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

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution n° 1 de la Conférence mondiale de normalisation des télécommunications (CMNT), (Helsinki, 1993). De plus, la CMNT, qui se réunit tous les quatre ans, approuve les Recommandations qui lui sont soumises et établit le programme d'études pour la période suivante.

Dans certains secteurs de la technologie de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI. Le texte de la Recommandation X.273 de l'UIT-T a été approuvé le 1er juillet 1994. Son texte est publié, sous forme identique, comme Norme internationale ISO/CEI 11577.

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.

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 syntax 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

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 applicables aux protocoles de couche réseau en mode connexion et en mode sans connexion. 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 défini par la présente Recommandation de l'UIT-T | Norme internationale est utilisé pour assurer des services de sécurité servant de support à une instance de communication entre des entités de couche inférieure. Ce protocole se caractérise, relativement aux autres normes, par la structure en couches définie dans la Rec. X.200 du CCITT | ISO 7498 ainsi que par l'organisation de la couche réseau définie dans ISO 8648 et étendue par la Rec. X.802 de l'UIT-T | TR 13595 (modèle de sécurité de couche inférieure). Il permet la mise en œuvre de services de sécurité servant de support à des services de réseau en mode connexion et sans connexion. Sa particularité est d'être situé dans la couche réseau et d'avoir des interfaces fonctionnelles ainsi que des interfaces de service nettement définies à ses limites supérieure et inférieure.

Pour évaluer la conformité d'une application particulière, il est nécessaire d'avoir une déclaration précisant quelles capacités et options ont été mises en œuvre pour un protocole OSI donné. Une telle déclaration est appelée déclaration de conformité d'une instance de protocole (PICS).

NORME INTERNATIONALE

RECOMMANDATION UIT-T

TECHNOLOGIES DE L'INFORMATION – INTERCONNEXION DES SYSTÈMES OUVERTS – PROTOCOLE DE SÉCURITÉ DE LA COUCHE RÉSEAU

1 Objet et domaine d'application

La présente Recommandation de l'UIT-T | Norme internationale spécifie un protocole qui doit être utilisé par les systèmes d'extrémité et les systèmes intermédiaires pour assurer des services de sécurité dans la couche réseau définie par la Rec. X.213 du CCITT | ISO 8348 ainsi que par ISO 8348 AD2 et ISO 8648. Le protocole défini dans la présente Recommandation de l'UIT-T | Norme internationale est appelé protocole de sécurité de couche réseau (NLSP).

La présente Recommandation de l'UIT-T | Norme internationale spécifie:

1) La mise en œuvre des services de sécurité suivants définis dans la Rec. X.800 du CCITT | ISO 7498-2:
   a) authentification de l'entité homologue;
   b) authentification de l'origine des données;
   c) contrôle d'accès;
   d) confidentialité des données en mode connexion;
   e) confidentialité des données en mode sans connexion;
   f) confidentialité du flux de trafic;
   g) intégrité en mode connexion sans reprise (y compris intégrité des unités de données, dans laquelle l'intégrité de chaque SDU est protégée au cours d'une connexion);
   h) intégrité en mode sans connexion.
2) Les caractéristiques fonctionnelles requises pour les applications déclarées conformes à la présente Recommandation de l'UIT-T | Norme internationale.

Les procédures du présent protocole sont définies en termes de:

a) conditions requises pour les techniques cryptographiques qui peuvent être utilisées dans une instance de ce protocole;
b) conditions requises pour les informations acheminées dans l'association de sécurité utilisée dans une instance de communication.

Bien que le degré de protection offert par certains mécanismes de sécurité dépende de l'utilisation de certaines techniques cryptographiques, la mise en œuvre correcte du présent protocole ne dépend pas du choix d'un algorithme de codage ou de décodage particulier. Ce choix doit faire l'objet d'une décision locale au niveau des systèmes de communication.

En outre, ni le choix ni l'application d'une politique de sécurité particulière n'entrent dans le cadre de la présente Recommandation de l'UIT-T | Norme internationale. Il incombe aux autorités locales de choisir une politique de sécurité particulière, donc le degré de protection qui sera assuré, parmi les systèmes qui utilisent une seule instance de communication sûre. La présente Recommandation de l'UIT-T | Norme internationale n'implique nullement que de multiples instances de communication sûres faisant intervenir un seul système ouvert doivent utiliser le même protocole de sécurité.

L'Annexe D décrit le formulaire PICS pour le protocole de sécurité de couche réseau conformément aux directives pertinentes données dans ISO/CEI 9646-2.

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 de l'UIT-T | 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 de l'UIT-T | Norme internationale

sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et Normes indiquées ci-après. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur. Le Bureau de 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 X.213 du CCITT (1992) | ISO 8348:1993, *Technologie de l'information – Définition du service de réseau pour l'interconnexion de systèmes ouverts.*
- Recommandation UIT-T X.233 (1993) | ISO/CEI 8473:1994, *Technologie de l'information – Protocole assurant le service réseau en mode sans connexion de l'interconnexion de systèmes ouverts: Spécification du protocole*.
- Recommandation UIT-T X.802 (1994) | ISO/CEI TR 13594:1994, *Technologie de l'information – Interconnexion de systèmes ouverts – Modèle de sécurité des couches inférieures*.
- Recommandation UIT-T X.803 (1994) | ISO/CEI TR 10745:1993, *Technologie de l'information – Interconnexion de systèmes ouverts – Modèle de sécurité des couches supérieures*.

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

- Recommandation X.200 du CCITT (1988), *Technologie de l'information – Interconnexion de systèmes ouverts – Mode de référence: Modèle de référence de base*.

  ISO 7498:1984, *Systèmes de traitement de l'information – Interconnexion de 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 de systèmes ouverts – Modèle de référence de base – Partie 2: Architecture de sécurité*.
- Recommandation X.210 du CCITT (1988), *Traitement de l'information – Interconnexion de systèmes ouverts – Conventions pour la définition de services OSI.*

  ISO/TR 8509:1987, *Système de traitement de l'information – Interconnexion de systèmes ouverts – Conventions de service OSI.*
- Recommandation X.209 du CCITT (1988), *Spécification des règles de codage de base pour la notation de syntaxe abstraite numéro un (ASN.1)*.

  ISO/CEI 8825:1990, *Technologie de l'information – Interconnexion de systèmes ouverts – Spécification de règles de base pour coder la notation de syntaxe abstraite numéro un (ASN.1)*.
- Recommandation X.223 du CCITT (1988), *Utilisation du protocole X.25 pour mettre en œuvre le service de réseau en mode connexion de l'OSI*.

  ISO/CEI 8878:1992, *Technologie de l'information – Communication de données – Utilisation du protocole X.25 pour fournir le service de réseau OSI en mode connexion*.
- Recommandation X.290 du CCITT (1992), *Cadre général et méthodologie des tests de conformité OSI pour les Recommandations sur les protocoles pour les applications du CCITT – Concepts généraux*.

  ISO/CEI 9646-1:1991, *Technologie de l'information – Interconnexion de systèmes ouverts – Essais de conformité – Méthodologie générale et procédures – Partie 1: Concepts généraux*.
- Recommandation X.291 du CCITT (1992), *Cadre général et méthodologie des tests de conformité OSI pour les Recommandations sur les protocoles pour les applications du CCITT – Spécification des suites de tests abstraites*.

  ISO/CEI 9646-2:1991, *Technologie de l'information – Interconnexion de systèmes ouverts – Essais de conformité – Méthodologie générale et procédures – Partie 2: Spécification des suites de tests abstraites.*
- Recommandation X.509 du CCITT (1988), *Technologie de l'information – Interconnexion de systèmes ouverts – L'annuaire: Cadre d'authentification*.

  ISO/CEI 9594-8:1990, *Technologie de l'information – Interconnexion de systèmes ouverts – L'annuaire – Partie 8: Cadre général d'authentification*.

2.3 Références additionnelles

- ISO/CEI 7498/AD1:1987, *Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Modèle de référence de base-Additif 1 – Transmission en mode sans connexion*.
- ISO 8648:1988, *Systèmes de traitement de l'information – Communication de données – Organisation interne de la couche réseau*.
- ISO/CEI 8208:1990, *Technologie de l'information – Communication de données – Protocole X.25 de couche paquets pour terminal de données*.
- ISO/CEI 9834-1:1993, *Technologie de l'information – Interconnexion de systèmes ouverts – Procédures pour des organismes d'enregistrement particuliers – Partie 1: Procédures générales*.
- ISO/CEI 9834-3:1990, *Technologie de l'information – Interconnexion de 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*.
- ISO/CEI 9979:1991, *Technologie de l'information – Techniques cryptographiques – Procédures pour l'enregistrement des algorithmes cryptographiques*.
- Recommandation X.25 du CCITT (1993), *Interface entre équipement terminal de données et équipement de terminaison du circuit de données pour terminaux fonctionnant en mode paquet et raccordés par circuit spécialisé à des réseaux publics pour données*.

3 Définitions

3.1 Définitions du modèle de référence

La présente Recommandation | Norme internationale utilise les termes suivants définis dans la Rec. X.200 du CCITT | ISO 7498:

a) système d'extrémité;

b) entité de réseau;

c) couche réseau;

d) protocole de réseau;

e) unité de données de protocole de réseau;

f) relais de réseau;

g) service de réseau;

h) point d'accès au service de réseau;

i) adresse de point d'accès au service de réseau;

j) unité de données de service de réseau;

k) unité de données de protocole;

l) routage;

m) service;

n) unité de données de service.

3.2 Définitions de l'architecture de sécurité

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

a) contrôle d'accès;

b) confidentialité;

c) intégrité en mode connexion sans reprise;

d) confidentialité des données en mode sans connexion;

e) intégrité en mode sans connexion;

f) authentification de l'origine des données;

g) décodage;

h) signature numérique;

i) codage;

j) authentification de l'entité homologue;

k) étiquette de sécurité;

l) service de sécurité;

m) confidentialité du flux de données.

3.3 Définitions des conventions de service

La présente Recommandation | Norme internationale utilise les termes suivants définis dans la Rec. X.210 du CCITT | ISO TR 8509:

a) fournisseur de service;

b) utilisateur de service.

3.4 Définitions du service de réseau

La présente Recommandation | Norme internationale utilise les termes suivants définis dans la Rec. X.213 du CCITT | ISO 8348:

– point de rattachement au sous-réseau.

3.5 Définitions de l'organisation interne de la couche réseau

La présente Recommandation | Norme internationale utilise les termes suivants définis dans ISO 8648:

a) système intermédiaire;

b) système relais;

c) sous-réseau;

d) protocole d'accès au sous-réseau;

e) protocole de convergence dépendant du sous-réseau;

f) protocole de convergence indépendant du sous-réseau.

3.6 Définitions du protocole de réseau en mode sans connexion

La présente Recommandation | Norme internationale utilise les termes suivants définis dans la Rec. UIT-T X.233 | ISO 8473:

a) PDU initiale;

b) décision locale;

c) réassemblage;

d) segment.

3.7 Définitions du modèle de sécurité de couche supérieure

La présente Recommandation | Norme internationale utilise les termes suivants définis dans la Rec. UIT-T X.803 | ISO/CEI 10745:

a) politique d'interaction sûre;

b) relation de sécurité.

3.8 Définitions des tests de conformité

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

a) formulaire PICS;

b) déclaration de conformité d'une instance de protocole;

c) revue de conformité statique.

3.9 Définitions additionnelles

Les définitions suivantes s'appliquent pour les besoins de la présente Recommandation | Norme internationale:

3.9.1 SA-ID bloqué: SA-ID non disponible pour assignation à une association de sécurité en raison de la nécessité d'empêcher sa réutilisation.

3.9.2 paire de clés: Paire de valeurs de clé liées (clé publique) ou identiques (clé secrète) pour utilisation entre deux correspondants particuliers.

3.9.3 information de commande de sécurité: Information de commande de protocole (PCI) échangée par un protocole de sécurité afin d'établir ou de maintenir une association de sécurité.

3.9.4 attributs SA: Ensemble d'informations requises pour commander la sécurité des communications entre une entité et son ou ses homologue(s) distante(s).

3.9.5 association de sécurité: Relation de sécurité entre des entités de couche inférieure communicantes et pour laquelle il existe des attributs SA correspondants.

3.9.6 intégrité d'unité de données: Forme d'intégrité de connexion dans laquelle l'intégrité de chaque SDU est protégée mais où les erreurs dans la séquence des SDU ne sont pas détectées.

3.9.7 dans la bande: Transmission effectuée par des mécanismes de protocole utilisant la SA PDU définie dans la présente Recommandation de l'UIT-T | Norme internationale.

3.9.8 hors bande: Transmission effectuée par des moyens autres que l'utilisation de la SA PDU.

3.9.9 règles de sécurité: Informations locales qui, compte tenu des services de sécurité sélectionnés, spécifient les mécanismes de sécurité à utiliser, y compris tous les paramètres nécessaires pour le fonctionnement des mécanismes.

NOTE – Ces informations peuvent faire partie des règles d'interaction de sécurité définies dans la Rec. X.803 du CCITT | ISO 10745.

3.9.10 étiquette: Voir «étiquette de sécurité» (Rec. X.800 du CCITT | ISO 7498-2).

4 Abréviations

4.1 Unités de données

NPDU	Unité de données de protocole de réseau (*network protocol data unit*)
NSDU	Unité de données de service de réseau (*network service data unit*)
PDU	Unité de données de protocole (*protocol data unit*)
SDU	Unité de données de service (*service data unit*)

4.2 Champs d'unité de données de protocole

LI	Indicateur de longueur (*length indicator*)

4.3 Paramètres

QOS	Qualité de service (*quality of service*)

4.4 Divers

ASSR	Ensemble mutuellement convenu de règles de sécurité (*agreed set of security rules*)
CL	Mode sans connexion (*connectionless mode*)
CLNP	Protocole de réseau en mode sans connexion (*connectionless mode network protocol*)
CLNS	Service de réseau en mode sans connexion (*connectionless mode network service*)
CO	Mode connexion (*connection mode*)
CSC PDU	PDU de commande de sécurité de connexion (*connection security control PDU*)

DU	Unité de données (*data unit*)
EKE	Echange de clés exponentielles (*exponential key exchange*) (voir l'Annexe H)
ES	Système d'extrémité (*end system*)
ICV	Valeur de contrôle d'intégrité (*integrity check value*)
IS	Système intermédiaire (*intermediate system*)
ISN	Numéro de séquence d'intégrité (*integrity sequence number*)
KEK	Clé de codage de clés (*key enciphering key*)
NLSP	Protocole de sécurité de couche réseau (*network layer security protocol*)
NLSP-CO	NLSP en mode connexion (*NLSP for connection mode*)
NLSP-CL	NLSP en mode sans connexion (*NLSP for connectionless mode*)
NLSPE	Entité de NLSP (*NLSP entity*)
NS	Service de réseau (*network service*)
NSAP	Point d'accès au service de réseau (*network service access point*)
PCI	Information de commande de protocole (*protocol control information*)
PDU	Unité de données de protocole (*protocol data unit*)
SA	Association de sécurité (*security association*)
SA-ID	Identificateur d'association de sécurité (*security association identifier*)
SA-P	Protocole d'association de sécurité (*security association protocol*)
SA PDU	PDU d'association de sécurité (*security association PDU*)
SCI	Information de commande de sécurité (*security control information*)
SDT-PDU	PDU de transfert de données sûres (*secure data transfer PDU*)
SN	Sous-réseau (*subnetwork*)
SNAcP	Protocole d'accès au sous-réseau (*subnetwork access protocol*)
SNICP	Protocole de convergence indépendant du sous-réseau (*subnetwork independent convergence protocol*)
SNPA	Point de rattachement au sous-réseau (*subnetwork point of attachment*)
UN	Réseau de base (*underlying network*)

5 Vue d'ensemble du protocole

5.1 Introduction

Il existe deux modes de mise en œuvre du protocole NLSP qui sont:

a) le NLSP-CL – Utilisé pour assurer un service de réseau sûr en mode sans connexion;

b) le NLSP-CO – Utilisé pour assurer un service de réseau sûr en mode connexion.

Les deux modes de protocole NLSP fonctionnent comme une sous-couche de la couche réseau. Le service fourni à l'entité située au-dessus est appelé service de NLSP et le service censé être fourni au protocole NLSP est appelé service de réseau de base (UN). Les préfixes UN et NLSP sont ajoutés aux primitives et aux paramètres pour distinguer clairement le service désigné. Les services UN et NLSP sont des «interfaces notionnelles», c'est-à-dire qu'ils sont décrits comme s'il s'agissait de services de couche mais résidaient potentiellement en totalité dans la couche réseau, selon l'emplacement occupé par la sous-couche de protocole NLSP (voir l'Annexe E).

Les deux modes de protocole NLSP peuvent être mis en œuvre dans des systèmes d'extrémité et dans des systèmes intermédiaires. Ils permettent tous deux de protéger, à titre facultatif, l'adresse NLSP d'origine et de destination ainsi que d'autres paramètres NLSP-CONNECT (connexion de NLSP). Le protocole NLSP-CO peut être mis en œuvre à un emplacement quelconque de la couche réseau. Le protocole NLSP-CL peut être mis en œuvre à un emplacement quelconque de la couche réseau au-dessus du protocole de convergence dépendant du sous-réseau (voir ISO 8648).

Le protocole est conçu de telle sorte qu'il puisse être optimisé pour répondre à un ensemble de conditions lorsque la préoccupation principale est d'assurer une haute sécurité dans des environnements où il s'agit d'obtenir le meilleur rendement possible des communications. Une option «no-header» (absence d'en-tête) dans laquelle l'incidence sur le rendement des communications est minimale bien que, éventuellement, avec une sécurité réduite, est notamment offerte dans le protocole NLSP-CO.

Le protocole NLSP est fondé sur le concept d'association de sécurité (SA) qui peut exister en dehors d'une primitive UNITDATA (unité de données) en mode sans connexion ou d'une connexion. Un ensemble d'attributs définissant des paramètres pour la sécurité (par exemple, algorithme, clés, etc.) est spécifié pour l'association SA.

Le protocole assure le même mode de service (CO ou CL) à ses limites supérieure et inférieure.

Le protocole permet d'utiliser un large éventail de mécanismes de sécurité particuliers (normalisés et non normalisés). Les utilisateurs et les réalisateurs doivent choisir, pour utilisation avec ce protocole, les mécanismes de sécurité appropriés pour assurer leur service de sécurité et le niveau de protection nécessaire. Les articles 9 à 12 et l'Annexe C définissent le mode de mise en œuvre d'un ensemble de mécanismes particuliers pour tous les services de sécurité nécessaires au protocole NLSP.

La protection en matière de sécurité que le NLSP tente d'assurer découle des conditions de service de sécurité établies par l'autorité responsable du domaine de sécurité.

NOTE – L'utilisation du paramètre QOS de protection du service NLSP est un problème d'ordre local qui sort du cadre de la présente Recommandation de l'UIT-T | Norme internationale.

5.2 Vue d'ensemble des services assurés

Le protocole NLSP assure les services de sécurité définis dans la Rec. X.800 du CCITT | ISO 7498-2 comme étant appropriés à la couche réseau ainsi que les services de couche de réseau OSI définis dans la Rec. X.213 du CCITT | ISO 8348 et ISO 8348/AD1.

Le protocole NLSP-CL permet d'assurer les services de sécurité suivants s'ils sont sélectionnés:

a) authentification de l'origine des données;

b) contrôle d'accès;

c) confidentialité des données en mode sans connexion. Cette protection inclut, à titre facultatif, tous les paramètres de service NLSP selon les services de sécurité sélectionnés;

d) confidentialité du flux de trafic;

e) intégrité en mode sans connexion. Cette protection inclut, à titre facultatif, tous les paramètres de service NLSP selon les services de sécurité sélectionnés.

Le protocole NLSP-CO permet d'assurer les services de sécurité suivants s'ils sont sélectionnés:

a) authentification de l'entité homologue;

b) contrôle d'accès;

c) confidentialité des données en mode connexion. Cette protection inclut, à titre facultatif, tous les paramètres de connexion NLSP selon les services de sécurité sélectionnés;

d) confidentialité du flux de trafic;

e) intégrité en mode connexion sans reprise. Cette protection inclut, à titre facultatif, tous les paramètres de connexion NLSP selon les services de sécurité sélectionnés. Elle inclut également, à titre facultatif, l'intégrité d'une séquence d'unités SDU.

5.3 Vue d’ensemble des services implicites

Les services implicites situés au-dessous du protocole NLSP sont appelés services de réseau de base (UN). Les services de base assurés implicitement par le protocole NLSP-CL utilisent les mêmes primitives que celles définies dans le service de réseau en mode sans connexion (Rec. X.213 du CCITT | ISO 8348/AD1).

Pour le protocole NLSP-CO, l'interface UN est modélisée en deux parties:

a) un service utilisant les mêmes primitives que celles de la Rec. X.213 du CCITT | ISO 8348 avec, en outre, un paramètre appelé paramètre d'authentification UN;

b) la mise en correspondance de ce service avec le service de réseau normalisé ou directement avec la Rec. X.25 du CCITT | ISO 8208.

L'adresse de réseau acheminée dans les primitives NLSP est appelée adresse NLSP. Ce paramètre de service identifie l'entité d'utilisateur NLSP qui peut être ou non une entité de transport selon que d'autres protocoles de couche réseau sont utilisés au-dessus du protocole NLSP ou que l'entité NLSP (NLSPE) est située dans un système d'extrémité (ES) ou un système intermédiaire (IS). L'adresse de réseau transmise au réseau de base est appelée adresse UN. Ce paramètre UN équivaut à l'adresse SNPA si, et seulement si, aucun protocole n'est mis en œuvre entre l'entité NLSP et l'entité d'accès au sous-réseau.

5.4 Associations de sécurité et règles de sécurité

5.4.1 Associations de sécurité

La mise en œuvre du protocole NLSP est commandée par un ensemble d'informations de gestion de sécurité (par exemple, informations de sélection de services de sécurité, identificateur d'algorithme de sécurité, clés cryptographiques) appelées attributs d'association de sécurité (attributs SA). L'ensemble d'attributs d'association de sécurité nécessaires pour gérer la fourniture de services de sécurité entre les entités communicantes est appelé association de sécurité.

Les associations de sécurité sont décrites d'une manière plus détaillée dans la Rec. UIT-T X.802 | ISO/CEI TR 13594 (modèle de sécurité des couches inférieures).

Les attributs SA nécessaires pour les deux protocoles NLSP-CL et NLSP-CO sont définis au 6.2. Les attributs SA nécessaires pour le protocole NLSP-CL sont définis au 7.4. Les attributs SA nécessaires pour le protocole NLSP-CO sont définis au 8.4. D'autres attributs spécifiques des mécanismes sont définis aux 10.2, 11.2 et 12.2.

Pour protéger une instance de communication (une SDU en mode sans connexion ou une connexion), on utilise une association SA appropriée existante ou, s'il n'existe aucune association SA appropriée, il faut en établir une entre les correspondants qui communiquent.

L'association de sécurité peut être établie hors bande ou à l'aide du protocole SA-P dans la bande du NLSP. Le protocole NLSP SA-P échange des informations de commande de sécurité (SCI) en utilisant des SA PDU et/ou SDT PDU avec type de données SA-P. Il convient d'utiliser des SA PDU si les informations SCI doivent être acheminées en clair et des SA PDU ou SDT PDU si les informations SCI doivent être protégées. Ces informations SCI sont utilisées pour établir les attributs SA en se fondant sur tout attribut SA et toute règle de sécurité préétablis.

Le protocole NLSP-CO permet également l'échange d'informations pour mettre à jour les attributs SA «dynamiques» (par exemple, clés actives, voir l'Annexe G) lors de l'établissement d'une connexion et au cours d'une connexion. La mise à jour des attributs SA dynamiques ne doit pas modifier les services de sécurité assurés.

L'utilisation d'un protocole SA-P dans la bande conjointement avec le protocole NLSP-CL est définie au 7.5. L'utilisation d'un protocole SA-P dans la bande avec le protocole NLSP-CO est définie aux 8.5 (phase d'établissement de la connexion) et 8.11.1 (phase de transfert de données). Un protocole pour la mise en œuvre du SA-P dans la bande est défini dans l'Annexe C de la présente Spécification. Un exemple de mécanisme d'établissement d'une clé destinée à être utilisée avec ce protocole est donné dans l'Annexe H.

5.4.2 Règles de sécurité

La détermination d'un certain nombre d'attributs SA sera soumise à des restrictions liées à la politique de sécurité. Cette partie de la politique de sécurité est appelée ensemble de règles de sécurité pour l'entité de protocole. L'ensemble de règles de sécurité pour une entité de protocole peut exiger que des attributs SA tels que les longueurs de champ, les algorithmes de codage, etc., n'aient qu'une seule et unique valeur ou qu'un ensemble de valeurs fasse l'objet de restrictions supplémentaires imposées par d'autres moyens (par exemple, gestion de systèmes OSI ou échange de données de protocole SA-P).

Lorsque plusieurs niveaux de protection sont offerts, l'ensemble de règles de sécurité définira les restrictions applicables en fonction des différentes qualités de protection nécessaires.

Lorsqu'on le met en œuvre entre des entités NLSPE, il faut, pour cet ensemble de règles de sécurité, établir un identificateur unique appelé ensemble mutuellement convenu de règles de sécurité (ASSR). L'identificateur ASSR peut être échangé lors de l'établissement de l'association de sécurité.

Les règles de sécurité sont décrites d'une manière plus détaillée dans TR 13594 (modèle de sécurité des couches inférieures).

5.5 Vue d'ensemble du protocole – Fonctions de protocole

5.5.1 Portée de la protection

Le protocole NLSP-CO et le protocole NLSP-CL ont chacun trois modes de fonctionnement différents qui assurent trois degrés fondamentaux de protection.

a) *Protection de tous les paramètres de service NLSP*

Dans ce mode, tous les paramètres de service NLSP, y compris les adresses et toutes les données d'utilisateur, mais à l'exception de ceux qui sont négociés avec le fournisseur de service (QOS, sélection de confirmation de réception, sélection de données exprès), sont protégés.

Ce mode est sélectionné par l'attribut SA Param_Prot (voir 6.2) réglé à la valeur VRAI.

b) *Protection des données d'utilisateur NLSP*

Dans ce mode, les données d'utilisateur sont protégées mais les autres paramètres de service NLSP ne le sont pas.

Ce mode est sélectionné par l'attribut SA Param_Prot réglé à la valeur FAUX.

Pour le protocole NLSP-CO, il existe d'autres sous-modes de protection des données d'utilisateur NLSP, à savoir:

1) toutes les données d'utilisateur NLSP sont protégées (y compris les données d'utilisateur NLSP dans les primitives de service NLSP-CONNECT (connexion NLSP), NLSP-DATA (données NLSP) et NLSP-DISCONNECT (déconnexion NLSP); ou

2) les données d'utilisateur NLSP dans la primitive NLSP-DATA sont protégées.

Les sous-modes pour le NLSP sont sélectionnés en outre par un attribut SA Protect_Connect_Params (voir 8.3). Si l'attribut Protect_Connect_Params est VRAI, toutes les données d'utilisateur NLSP sont protégées, sinon seules les données d'utilisateur NLSP dans la primitive NLSP-DATA sont protégées. L'attribut Protect_Connect_Params sera forcé à la valeur VRAI (c'est-à-dire que toutes les données d'utilisateur NLSP seront protégées) si l'attribut Param_Prot est VRAI.

c) *Aucune protection*

Dans ce mode, tous les paramètres de service NLSP sont directement copiés dans les paramètres de service UN équivalents. Toutes les procédures du protocole NLSP sont court-circuitées.

Ce mode est sélectionné localement en fonction des adresses des entités homologues qui communiquent et des exigences du service de sécurité local.

5.5.2 Qualité de la protection

La qualité de service (QOS) en matière de sécurité (protection) dans les couches inférieures OSI est obtenue par la sélection, au niveau de la mise en œuvre, des services de sécurité qui doivent être assurés dans le cadre de la politique de sécurité localement gérée. Toute indication, dans la bande, de services de sécurité sélectionnés est acheminée dans un protocole d'association de sécurité indépendant d'une instance de communication, cette indépendance étant assurée implicitement par l'utilisation d'une étiquette de sécurité ou explicitement par d'autres moyens. En conséquence, tout échange relatif à la sélection de services de sécurité est indépendant de l'acheminement de paramètres QOS entre les limites d'interface de service.

NOTE – Il peut être également nécessaire d'indiquer les services de sécurité aux couches supérieures. Cependant, aucune nécessité immédiate de définir des caractéristiques particulières de QOS en matière de protection n'a été établie jusqu'ici.

5.5.3 Fonction de protection de données

5.5.3.1 Protection fondée sur les SDT PDU

Les deux protocoles NLSP-CO et NLSP-CL peuvent protéger les paramètres de service NLSP en utilisant une PDU de transfert de données sûres (SDT PDU). Le protocole NLSP-CO a également un autre moyen de protection des données d'utilisateur NLSP qui est sélectionné par l'attribut SA No_Header (voir 8.3) réglé à la valeur VRAI.

Les procédures fondées sur la SDT PDU permettent de protéger les paramètres de service NLSP:

a) en codant les paramètres de service NLSP sous la forme d'un champ «Octet-String-Before-Encapsulation» (chaîne d'octets avant encapsulation);

b) en plaçant une étiquette de sécurité dans le champ «Octet-String-Before-Encapsulation» si l'étiquetage de sécurité explicite est sélectionné (l'étiquette d'attribut SA est réglée à la valeur VRAI);

c) en appliquant une fonction d'encapsulation (et de désencapsulation) qui permet la mise en œuvre de mécanismes pour assurer:

– la confidentialité du flux de trafic;

– l'intégrité et l'authentification de l'origine des données;

– la confidentialité,

selon les services de sécurité sélectionnés. Cette fonction permet d'obtenir une chaîne d'octets protégée.

Les paragraphes 6.4.1.1 et 6.4.2.1 définissent des procédures générales, indépendantes des mécanismes, pour l'utilisation de la SDT PDU en vue de la protection des données. L'article 11 définit la mise en œuvre d'une classe de mécanisme pour l'encapsulation fondée sur la SDT PDU. D'autres procédures d'encapsulation définies à titre privé peuvent être utilisées avec la SDT PDU.

5.5.3.2 Mode No_Header (protocole NLSP-CO seulement)

Le mode No_Header du protocole NLSP protège la primitive NLSP Userdata par une fonction d'encapsulation qui ne modifie pas la longueur des données protégées. Le protocole NLSP n'ajoute aucune information de commande de protocole aux données protégées. Les services de sécurité mis en œuvre dépendent des mécanismes utilisés mais la fonction d'encapsulation doit au moins assurer la confidentialité. Le mode No_Header ne peut être utilisé que pour protéger un seul paramètre de service (NLSP Userdata) et donc dans le cas où l'attribut Param_Prot est réglé à la valeur FAUX.

Les paragraphes 6.4.1.2 et 6.4.2.2 définissent des procédures générales, indépendantes des mécanismes, pour l'utilisation du mode No_Header en vue de la protection des données. L'article 12 définit la mise en œuvre d'une classe de mécanisme pour l'encapsulation de l'attribut SA No_Header. D'autres procédures d'encapsulation définies à titre privé peuvent être utilisées avec le mode No_Header.

5.5.4 Commande de sécurité de connexion (protocole NLSP-CO seulement)

Lors de l'établissement d'une connexion, des PDU de commande de sécurité de connexion sont échangées pour signaler le mode d'établissement de connexion NLSP [que ce soit avec un protocole SA-P dans la bande ou que les primitives NLSP-CONNECT soient mises en correspondance avec les primitives UN-CONNECT (connexion de réseau de base) ou UN-DATA (données de réseau de base)]. En outre, la CSC PDU peut assurer l'authentification de l'entité homologue et établir des valeurs pour les attributs SA dynamiques tels que les clés et les numéros de séquence d'intégrité, ce qui permet de réutiliser une association SA préalablement établie sans être obligé de recourir au protocole SA-P. La CSC PDU peut être également utilisée au cours d'une connexion pour authentifier à nouveau l'association SA (prouver que la connaissance de cette association SA est partagée) ou pour mettre à jour les attributs dynamiques.

La CSC PDU n'est utilisée que dans le protocole NLSP en mode connexion. L'article 8 définit les procédures générales, indépendantes des mécanismes, pour l'utilisation de la CSC PDU. L'article 10 définit la mise en œuvre d'une classe de mécanisme pour l'authentification et la gestion des clés. D'autres procédures définies à titre privé pour la mise en œuvre d'autres classes de mécanisme peuvent être utilisées avec la CSC PDU.

NOTE – Lorsqu'on utilise d'autres mécanismes d'authentification, ceux-ci doivent établir une valeur initiale pour le numéro ISN si le mécanisme ISN défini à l'article 11 est sélectionné.

5.5.5 PDU utilisées par le protocole NLSP

Les PDU suivantes sont utilisées par le protocole NLSP:

a) *PDU de transfert de données sûres* – Pour protéger les paramètres des primitives de service NLSP et d'autres données par encapsulation comme indiqué au 5.5.3.1. La structure de cette PDU est définie au 13.3.

b) *PDU de commande de sécurité de connexion* – Pour commander le mode d'établissement de connexion NLSP-CO et assurer, à titre facultatif, l'authentification de l'entité homologue ainsi que pour modifier les attributs SA dynamiques comme indiqué au 5.5.4. La structure de cette PDU est définie au 13.5.

NOTE – La CSC PDU n'est applicable qu'au protocole NLSP-CO.

c) *SA PDU* – PDU qui permet l'échange, dans la bande, d'informations de commande de sécurité pour les besoins de la gestion d'associations SA comme indiqué au 5.4.1. La structure de cette PDU est définie au 13.4.

En outre, avec le protocole NLSP-CO, les données peuvent être protégées, à titre facultatif, sans adjonction d'aucune information de commande de protocole supplémentaire (c'est-à-dire sans utilisation de la SDT PDU), comme indiqué au 5.5.3.2.

5.6 Vue d'ensemble du protocole – NLSP-CL

5.6.1 Paragraphes définissant le protocole NLSP-CL

Les procédures pour le protocole NLSP-CL sont définies aux articles 6 et 7 et les procédures facultatives d'encapsulation spécifiques des mécanismes à l'article 11. Ces procédures utilisent la SDT PDU définie au 13.3 et, à titre facultatif, la SA PDU définie au 13.4.

Les paragraphes qui suivent ne donnent qu'une vue d'ensemble du fonctionnement du protocole NLSP-CL, celui-ci étant décrit plus spécifiquement dans les paragraphes indiqués ci-dessus.

5.6.2 Fonctions du protocole NLSP-CL

Le protocole NLSP offre la possibilité de transférer, en mode sans connexion, des données protégées ou non protégées entre des utilisateurs NLSP homologues si les règles de contrôle d'accès de l'ASSR le permettent. La NLSPE détermine localement (à l'aide des services de sécurité sélectionnés, de l'adresse NLSP de destination et d'autres informations de gestion) si une protection est nécessaire ou non. Le transfert de données protégées peut s'effectuer avec la protection de tous les paramètres de service NLSP ou seulement des données d'utilisateur NLSP, le mode de protection étant déterminé par l'attribut SA Param_Prot.

A la réception d'une demande NLSP-UNITDATA:

- l'entité NLSP vérifie l'association SA; elle détermine si une communication non protégée avec l'adresse de destination est autorisée et, dans l'affirmative, si une protection est nécessaire;
- si aucune protection n'est nécessaire, l'entité NLSP copie toutes les primitives et tous les paramètres NLSP dans les primitives et les paramètres UN correspondants sans changement;
- si une protection est nécessaire, l'entité NLSP encapsule les paramètres de service, crée une SDT PDU et la transfère sous la forme de données d'utilisateur UN d'une demande UN-UNITDATA avec l'adresse d'origine UN, l'adresse de destination UN et les paramètres UN QOS (QOS du réseau de base). Cette procédure permet de protéger seulement les données d'utilisateur NLSP ou tous les paramètres de service NLSP.

A la réception de l'indication UN-UNITDATA, l'entité NLSP:

- utilise l'adresse d'origine UN et les informations locales pour déterminer si la communication avec l'adresse de destination est autorisée et, dans l'affirmative, si une protection est nécessaire;
- si une protection n'est pas nécessaire, les paramètres de service UN sont copiés dans les paramètres NLSP sans changement;
- si une protection est nécessaire, l'entité NLSP vérifie la SDT PDU, extrait les données d'utilisateur NLSP et, à titre facultatif, les autres paramètres de service NLSP en utilisant la fonction de désencapsulation. Les données d'utilisateur, l'adresse d'origine, l'adresse de destination et les paramètres QOS sont transmis à l'utilisateur NLSP dans l'indication NLSP-UNITDATA.

NOTE – A l'émission, le protocole NLSP peut fonctionner après (avant, à la réception) les fonctions de protocole CLNP de la Rec. UIT-T X.233 | ISO/CEI 8473 protégeant les CLNP PDU. De même, à l'émission, le protocole NLSP peut fonctionner avant (après, à la réception) les fonctions de protocole CLNP, les NLSP PDU étant acheminées dans les champs de données des CLNP PDU. Voir l'Annexe E pour de plus amples détails sur l'utilisation des protocoles NLSP et CLNP.

Etant donné que certains paramètres CLNP peuvent relever de la sécurité, la sélection de ces paramètres, après le protocole NLSP à l'émission, doit être effectuée en fonction de la politique de sécurité locale. Certains des paramètres facultatifs à prendre en considération sont l'enregistrement de la voie d'acheminement, le routage d'origine partiel et complet ainsi que le comptage des bonds. L'un quelconque de ces paramètres pourrait donner, sur un réseau, des informations qui ne doivent pas être communiquées à un observateur de ce réseau.

Pour déterminer qu'une NLSP-CL PDU a été acheminée dans une CLNP PDU, à la réception, le destinataire doit vérifier que le sélecteur de l'adresse de destination ne contient que des zéros ou que l'identificateur de protocole NLSP dans le champ de données de la CLNP PDU est tel que défini au 13.3. L'une ou l'autre vérification peut être utilisée pour indiquer que cette PDU doit être traitée par la couche réseau ou être envoyée directement à la couche transport.

5.7 Vue d'ensemble du protocole – NLSP-CO

5.7.1 Paragraphes définissant le NLSP-CO

Les procédures pour le protocole NLSP-CO fondées sur l'attribut No_Header sont définies aux articles 6 et 8, les procédures facultatives spécifiques des mécanismes à l'article 12 pour l'encapsulation et à l'article 10 pour la commande de sécurité de connexion. Ces procédures utilisent la CSC PDU définie au 13.5 et, à titre d'option, la SA PDU définie au 13.4.

Les procédures pour le protocole NLSP-CO fondées sur l'utilisation de la SDT PDU sont définies aux articles 6 et 8, les procédures facultatives spécifiques des mécanismes à l'article 11 pour l'encapsulation et à l'article 10 pour la commande de sécurité de connexion. Ces procédures utilisent la SDT PDU définie au 13.3, la CSC PDU définie au 13.5 et, à titre d'option, la SA PDU définie au 13.4.

Les paragraphes qui suivent ne donnent qu'une vue d'ensemble du fonctionnement du protocole NLSP-CO, celui-ci étant décrit plus spécifiquement dans les paragraphes indiqués ci-dessus.

5.7.2 Connexions non protégées du protocole NLSP-CO

Si des communications non protégées sont autorisées entre les adresses appelante et appelée, tous les paramètres de service NLSP/UN sont copiés directement de l'interface de service NLSP vers l'interface de service UN et vice versa.

5.7.3 Fonction NLSP-CONNECT (connexion NLSP)

A la réception d'une demande NLSP-CONNECT, la NLSPE vérifie s'il existe une association SA applicable avec les caractéristiques requises. Dans l'affirmative, cette association SA peut être utilisée pour protéger la connexion. Dans le cas contraire, une nouvelle SA est établie dans la bande, dans le cadre des fonctions NLSP-CONNECT, ou hors bande dans un délai donné. Si ni l'une ni l'autre de ces fonctions ne peut être exécutée, une primitive NLSP-DISCONNECT est renvoyée.

Deux modes fondamentaux d'établissement d'une connexion NLSP sont mis en œuvre. Dans le premier, les paramètres NLSP-CONNECT sont acheminés dans les primitives de service UN-CONNECT. Dans le second, les paramètres NLSP-CONNECT sont acheminés, après avoir été encapsulés dans une SDT PDU, dans la primitive UN-DATA après l'établissement de la connexion UN. Il existe des variantes de ces deux modes d'établissement de connexion NLSP, l'une pour utilisation avec des échanges, dans la bande, de données de protocole SA-P (à l'aide de la SA PDU et/ou SDT PDU avec type de données SA-P) acheminées dans la primitive UN-DATA, l'autre pour utilisation avec une association SA qui a été établie hors bande.

La PDU commande de sécurité de connexion (CSC) est utilisée pour signaler le mode d'établissement de la connexion et, si un protocole SA-P n'est pas acheminé dans la bande, l'échange de CSC PDU est également utilisé:

a) pour établir des attributs de sécurité spécifiques des mécanismes destinés à protéger la connexion (par exemple, clés, numéros de séquence d'intégrité);

b) pour effectuer l'authentification de l'entité homologue.

L'article 10 définit la mise en œuvre facultative de mécanismes d'authentification simple fondée sur le concept sollicitation-réponse et de gestion des clés.

Dans le cas où les paramètres NLSP-CONNECT sont acheminés dans une primitive UN-CONNECT avec le protocole SA-P dans la bande, une connexion UN est établie pour acheminer le protocole SA-P puis est libérée avant l'échange de primitives UN-CONNECT acheminant les paramètres NLSP-CONNECT. Les CSC PDU sont utilisées lors du deuxième échange de primitives UN-CONNECT pour une nouvelle authentification des entités NLSP homologues.

L'établissement de l'association SA s'effectue par l'échange de SA PDU ou SDT PDU qui acheminent les informations nécessaires pour établir les attributs SA requis. L'Annexe C définit un protocole SA à cet effet.

S'il est nécessaire de protéger les paramètres NLSP-CONNECT, ils seront encapsulés avant leur transfert.

5.7.4 Fonction NLSP-DATA (données NLSP)

A la réception d'une demande NLSP-DATA:

a) si une protection fondée sur la SDT PDU est sélectionnée, l'entité NLSP encapsule les paramètres de service appropriés, crée une SDT PDU et la transfère sous la forme de données d'utilisateur UN d'une demande UN-DATA;

b) si une protection fondée sur l'attribut No_Header est sélectionnée, les données d'utilisateur NLSP sont codées et transférées sous la forme de données d'utilisateur UN d'une demande UN-DATA;

A la réception d'une indication UN-DATA:

a) si une protection fondée sur la SDT PDU est sélectionnée, l'entité NLSP vérifie la PDU et extrait les données d'utilisateur NLSP ainsi que, éventuellement une demande de confirmation NLSP en utilisant la fonction de désencapsulation;

b) si une protection fondée sur l'attribut No_Header est sélectionnée, les données d'utilisateur UN sont décodées pour obtenir les données d'utilisateur NLSP;

c) les paramètres de service NLSP sont transmis à l'utilisateur NLSP dans l'indication NLSP-DATA.

5.7.5 Fonction NLSP-EXPEDITED-DATA (données NLSP exprès)

Cette demande est traitée de la même façon qu'une demande NLSP-DATA.

NOTE – En cas d'utilisation de la SDT PDU, la fonction d'encapsulation peut accroître la longueur des données; compte tenu de la longueur restreinte du champ de données d'utilisateur, il peut donc être nécessaire de segmenter à nouveau et de réassembler les données exprès protégées lors de leur passage par le réseau de base.

5.7.6 Fonction NLSP-RESET

Cette demande est transmise directement au réseau de base par le protocole NLSP. La connexion sûre fait l'objet d'une nouvelle authentification et les attributs spécifiques des mécanismes sont réétablis à l'aide de CSC PDU acheminées dans la primitive UN-DATA.

NOTE – Il peut être également nécessaire de réinitialiser certains mécanismes de sécurité car des données ont pu être perdues. Des mécanismes de séquencement d'intégrité doivent, en particulier, pouvoir empêcher les attaques consistant à répéter des messages dans un but malveillant, même après la perte de données.

5.7.7 Fonction NLSP-DATA-ACKNOWLEDGE (accusé de réception de données NLSP)

Si tous les paramètres NLSP doivent être protégés (c'est-à-dire si l'attribut Param_Prot est réglé à la valeur VRAI), cette primitive est encapsulée, placée dans une SDT PDU et transmise à la sous-couche UN par le protocole NLSP. Dans le cas contraire, cette primitive de service est mise directement en correspondance avec la primitive UN-DATA-ACKNOWLEDGE (accusé de réception de données UN).

5.7.8 Fonction NLSP-DISCONNECT (déconnexion de NLSP)

A la réception d'une demande NLSP-DISCONNECT, si la protection des paramètres de service est exigée par le mode de protection sélectionné (voir 5.5.1), l'entité NLSP construit une PDU de transfert de données sûres contenant la demande NLSP-DISCONNECT, les données d'utilisateur NLSP et, à titre facultatif, les autres paramètres. Cette PDU est soit acheminée dans une primitive UN-DATA avant la libération de la connexion UN ou, s'il y a lieu, la SDT PDU peut être acheminée dans le paramètre UN Userdata d'une primitive UN-DISCONNECT.

Si la protection des paramètres de la demande NLSP-DISCONNECT n'est pas nécessaire, ces paramètres sont envoyés dans une demande UN-DISCONNECT.

5.7.9 Autres fonctions

Le protocole NLSP met également en œuvre les fonctions suivantes qui sont déclenchées à l'expiration d'une temporisation ou à l'occasion d'autres événements externes:

a) échange de CSC PDU pour modifier des attributs SA dynamiques tels que des clés;

b) échange de tests de sécurité pour vérifier que les aspects cryptographiques de l'association SA sont correctement établis;

c) transmission de SDT PDU ne contenant qu'un champ de remplissage de trafic pour la confidentialité du flux de trafic.

6 Fonctions de protocole communes aux protocoles NLSP-CL et NLSP-CO

6.1 Introduction

Le présent article décrit les fonctions de protocole communes aux protocoles NLSP en mode connexion et sans connexion. Ces fonctions sont utilisées comme indiqué aux articles 7 et 8.

6.2 Attributs SA communs

Les attributs SA suivants commandent la mise en œuvre du protocole NLSP en mode connexion et sans connexion. Leur description inclut la mnémonique utilisée pour se référer à ces attributs dans la présente Spécification.

NOTE – Lorsqu'un attribut SA est «imposé par l'ASSR», l'ASSR peut définir une seule valeur ou une série de valeurs. Lorsque l'ASSR définit une série de valeurs, la valeur de l'attribut peut être établie par la gestion des systèmes OSI, par un échange de données de protocole SA-P ou par d'autres moyens qui sortent du cadre de la présente Spécification.

a) *Identification d'association SA:*

My_SA-ID: nombre entier compris entre
0 et (256 ** longueur max.) – 1

Identificateur local de la SA. La valeur de cet attribut doit être fixée lors de l'établissement de la SA.

Your_SA-ID: nombre entier compris entre
0 et (256 ** longueur max.) – 1

Identificateur distant de la SA. La valeur de cet attribut doit être fixée lors de l'établissement de la SA.

La longueur maximale est un nombre entier compris entre 2 et 126.

NOTE 1 – L'attribution d'un même identificateur local à plusieurs associations SA est une action sérieusement erronée.

b) *Indicateur précisant si la NLSPE a déclenché l'établissement de l'association SA ou y a répondu:*

Entité appelante: Valeur booléenne

Cet attribut indique comment le marqueur «entité appelante vers entité appelée» doit être positionné pour la détection des PDU réfléchies.

La valeur de cet attribut doit être fixée lors de l'établissement de l'association SA.

c) *Adresse UN de la NLSP homologue:*

Peer_Adr: Chaîne d'octets au format défini dans la Rec. X.213 du CCITT | ISO 8348/AD2

La valeur de cet attribut doit être fixée lors de l'établissement de l'association SA.

d) *Adresse NLSP d'entités desservies par l'entité homologue distante:*

Adr_Served: Ensemble de chaînes d'octets au format défini dans la Rec. X.213 du CCITT | ISO 8348/AD2

La valeur de cet attribut doit être fixée lors de l'établissement de l'association SA ou préalablement.

e) *Services de sécurité sélectionnés pour l'association SA:*

AC: Nombre entier compris entre des limites imposées par l'ASSR

TF_Conf: Nombre entier compris entre des limites imposées par l'ASSR

f) *Protection de paramètres:*

Param_Prot: Valeur booléenne

Protéger tous les paramètres de service NLSP autres que ceux qui peuvent être modifiés par le réseau de base (c'est-à-dire QOS, sélection de confirmation de réception et sélection de données exprès).

g) *Attributs de mécanisme d'étiquetage:*

Label: Valeur booléenne

Etiquetage explicite de PDU en mode connexion/sans connexion

Label_Set: Ensemble de
{Label_Ref: Nombre entier
Label_Auth: Identificateur d'objet
Label_Content: au format défini par Label_Auth}

La valeur de ces attributs est fixée lors de l'établissement de l'association SA ou préalablement.

NOTE 2 – Il est prévu que ces étiquettes seront enregistrées conformément aux procédures définies par l'ISO/CEI et l'UIT-T.

6.3 Fonctions communes lors d'une demande d'instance de communication

6.3.1 Vérifications initiales

Une NLSPE qui reçoit une demande d'instance de communication (c'est-à-dire une demande NLSP-CONNECT ou UNITDATA) doit vérifier que:

a) l'adresse appelante ou d'origine de protocole NLSP est une adresse NLSP desservie par cette NLSPE;

b) les services de sécurité requis peuvent être assurés par cette NLSPE.

6.3.2 Identification de l'association de sécurité

Une NLSPE qui reçoit une demande d'instance de communication (c'est-à-dire une demande NLSP-CONNECT ou UNITDATA) identifie, parmi les associations SA disponibles, une association SA dont les attributs répondent aux conditions suivantes:

a) toutes les caractéristiques de service de sécurité déterminées localement correspondent aux services de sécurité sélectionnés pour l'association SA;

b) l'adresse appelée ou de destination du protocole NLSP est contenue dans l'ensemble d'adresses NLSP de l'attribut Adr_Served;

c) aucune connexion NLSP n'utilise actuellement cette association SA (protocole NLSP-CO seulement).

Les procédures à suivre, si plusieurs associations SA répondent à ces conditons, relèvent du domaine local. S'il n'existe aucune de ces associations SA et si l'établissement d'associations SA dans la bande est pris en charge, l'option SA-P (protocole SA) peut être sélectionnée comme indiqué aux articles 7 et 8. Dans le cas contraire, des procédures d'établissement d'association SA hors bande peuvent être suivies. Si ni l'une ni l'autre de ces procédures ne peut être appliquée avec succès dans un délai défini localement, des procédures de reprise d'erreur appropriées au mode de communication, comme indiqué aux 7.4 et 8.4, seront mises en œuvre.

6.4 Fonctions de protocole de transfert de données sûres

6.4.1 Emission

6.4.1.1 Fonctions fondées sur la SDT PDU

Les opérations suivantes doivent être exécutées comme indiqué aux articles 7 et 8:

a) le bit 8 du champ de type de données doit être réglé à la valeur de l'entité initiatrice de l'attribut SA;

b) si ces procédures sont invoquées conformément au 8.6 (NLSP-DATA), le bit 7 du champ de type de données doit être réglé conformément à ces procédures, sinon ce bit est réglé à une valeur indiquant «last» (champ complet);

c) les bits 1 à 6 du champ de type de données doivent être réglés à une valeur définie au 13.3.4.2, conformément aux procédures décrites aux articles 7 et 8;

d) les données relatives aux paramètres de service NLSP ou à d'autres échanges de protocole (par exemple, données de test) sont placées dans les champs de contenu appropriés (voir 13.3.4.3), conformément aux procédures définies aux articles 7 et 8;

e) si l'attribut Label est VRAI, et dans le cas du protocole NLSP-CO, il s'agit de la première SDT PDU envoyée sur la connexion en cours, donc:

   1) une étiquette de sécurité, y compris l'autorité de définition, doit être placée dans un champ de contenu d'étiquette et incluse dans la PDU; ou

   2) une référence d'étiquette de sécurité doit être placée dans un champ de contenu de référence d'étiquette et incluse dans la PDU.

   L'étiquette sélectionnée doit être l'une des valeurs de l'attribut SA Label_Set;

   NOTE 1 – Dans le cas du protocole NLSP-CO, si le paramètre Protect_Connect_Params est présent, seule la SDT PDU qui achemine les paramètres NLSP-CONNECT sera étiquetée, sinon la première SDT PDU envoyée dans l'un ou l'autre sens pendant la phase de transfert de données NLSP sera étiquetée.

f) une fonction d'encapsulation (par exemple, celle décrite à l'article 11) doit être appelée avec transmission des arguments suivants:

   1) l'identificateur SA-ID doit être réglé à la valeur My_SA-ID;

   2) le type d'unité de données doit être réglé à la valeur:

      - «exprès» si les données à protéger sont extraites d'une primitive NLSP-EXPEDITED-DATA;
      - «normal» dans le cas contraire;

   3) le champ Octet-String-Before-Encapsulation doit être réglé à la valeur des champs de PDU construits;

g) la fonction d'encapsulation doit renvoyer soit une erreur soit un champ encapsulated-octet-string (chaîne d'octets encapsulée). Lorsque la fonction d'encapsulation a été exécutée avec succès, l'en-tête non protégé de la SDT PDU doit être créé comme indiqué au 13.3.2, le champ encapsulated-octet-string étant ajouté à l'en-tête.

   NOTE 2 – L'identificateur SA-ID n'est pas présent dans le protocole NLSP-CO.

6.4.1.2 Attribut No Header présent (protocole NLSP-CO seulement)

Les opérations suivantes doivent être exécutées comme indiqué à l'article 8:

a) une fonction d'encapsulation qui ne modifie pas la longueur des données (par exemple, celle décrite à l'article 12) doit être appelée avec transmission des arguments suivants:

   1) l'identificateur SA-ID doit être réglé à la valeur My_SA-ID;

   2) le type d'unité de données doit être réglé à la valeur:

      - «exprès» si les données à protéger sont extraites d'une primitive NLSP-EXPEDITED-DATA;
      - «normal» dans le cas contraire;

   3) le champ Octet-String-Before-Encapsulation doit être réglé à la valeur du paramètre NLSP Userdata;

b) la fonction d'encapsulation doit renvoyer soit une erreur soit un champ encapsulated-octet-string.

6.4.2 Vérification

6.4.2.1 Vérification fondée sur la SDT PDU

Les opérations suivantes doivent être exécutées comme indiqué aux articles 7 et 8:

a) l'en-tête non protégé doit être rejeté de la PDU;

b) une fonction d'encapsulation (par exemple, celle décrite à l'article 11) doit être appelée avec transmission des arguments suivants:

   1) l'identificateur SA-ID doit être réglé à la valeur My_SA-ID;

   2) le type d'unité de données doit être réglé à la valeur:

      - «exprès» si les données à décapsuler sont extraites d'une primitive UN-EXPEDITED-DATA;
      - «normal» dans le cas contraire;

   3) le champ encapsulated-octet-string doit être réglé à la valeur des éléments restants de la PDU;

c) la fonction de désencapsulation doit renvoyer soit une erreur soit un champ Octet-String-Before-Encapsulation. Lorsque la fonction de décapsulation a été mise en œuvre avec succès, les opérations de traitement suivantes doivent être exécutées;

d) il convient de vérifier que le bit 8 du champ de type de données (marqueur entité appelante vers entité appelée) n'est PAS égal à la valeur de l'entité initiatrice de l'attribut SA;

e) il convient de vérifier que les bits 1 à 6 et le bit 7 du champ de type de données ont une valeur appropriée pour les procédures indiquées aux articles 7 et 8;

f) si l'attribut Label est VRAI, et dans le cas du protocole NLSP-CO, il s'agit de la première SDT PDU reçue sur la connexion en cours; il convient donc de vérifier la PDU pour s'assurer qu'un seul et unique champ de contenu d'étiquette ou de référence d'étiquette est présent. Si ce champ est présent, il convient de vérifier la valeur de l'étiquette pour s'assurer qu'elle est contenue dans l'ensemble Label_Set;

g) il convient de vérifier que les champs de contenu relatifs aux paramètres de service NLSP ou à d'autres fonctions de protocole sont présents conformément aux procédures des articles 7 et 8. Les données sont extraites de ces champs et traitées conformément aux procédures des articles 7 et 8.

6.4.2.2 Attribut No_Header présent (protocole NLSP-CO seulement)

Les opérations suivantes doivent être exécutées comme indiqué à l'article 8:

a) la fonction de désencapsulation définie comme devant être utilisée pour cette association SA (par exemple, celle décrite à l'article 12) doit être appelée avec transmission des arguments suivants:

   1) l'identificateur SA-ID doit être réglé à la valeur My_SA-ID;

   2) le type d'unité de données doit être réglé à la valeur:

      - «exprès» si les données à décapsuler sont extraites d'une primitive UN-EXPEDITED-DATA;
      - «normal» dans le cas contraire;

3) le champ encapsulated-octet-string doit être réglé à la valeur du paramètre UN Userdata;

b) la fonction de désencapsulation doit renvoyer soit une erreur soit un champ Octet-String-Before-Encapsulation.

6.5 Utilisation d'un protocole d'association de sécurité

Lorsque deux NLSPE n'ont pas d'association SA établie, elles peuvent en établir une en utilisant un protocole d'association de sécurité (SA-P) ou une autre méthode. Un protocole SA-P échange des SA PDU ou SDT PDU, avec type de données réglé à la valeur SA-P, entre des NLSPE pour établir, modifier ou terminer une association SA.

Les articles 7 et 8 relatifs au protocole NLSP définissent comment le protocole SA-P peut être invoqué mais ne décrivent aucune procédure SA-P. Les procédures applicables au protocole SA-P et aux informations PCI contenues dans la SA PDU/SDT PDU dépendent du mécanisme particulier utilisé pour mettre en œuvre le protocole SA-P (un mécanisme de protocole approprié est défini dans l'Annexe C). Tout protocole SA-P doit présenter les caractéristiques suivantes:

a) détermination de tous les attributs SA nécessaires pour la forme de protection sélectionnée;

b) clés provenant d'une source authentifiée;

c) établissement d'informations initiales à des fins d'authentification et d'intégrité, si nécessaire.

Une NLSPE doit rejeter les SA PDU si le protocole SA-P spécifique n'est pas pris en charge.

Un protocole SA-P peut être fondé sur des algorithmes symétriques ou asymétriques. Il est recommandé d'utiliser un algorithme asymétrique. L'Annexe C contient un exemple de ce mécanisme.

7 Fonctions de protocole pour le protocole NLSP-CL

7.1 Services assurés par le protocole NLSP-CL

Les services assurés par le protocole NLSP seront désignés par le préfixe «NLSP». Les primitives sont les suivantes:

Primitives	*Paramètres*
NLSP-UNITDATA Request	Adresse de destination NLSP
(demande d'unité de données NLSP)	Adresse d'origine NLSP
NLSP-UNITDATA Indication	Qualité de service NLSP
(indication d'unité de données NLSP)	Données d'utilisateur NLSP

Les primitives et les paramètres de service sont directement équivalents à ceux définis dans la Rec. X.213 du CCITT | ISO 8348/AD1.

7.2 Services implicites

Les services implicitement assurés par le protocole NLSP à sa limite inférieure seront désignés par le préfixe «UN» (pour «réseau de base»). Les primitives sont les suivantes:

Primitives	*Paramètres*
UN-UNITDATA Request	Adresse UN appelée
(demande d'unité de données UN)	Adresse UN appelante
UN-UNITDATA Indication	Qualité de service UN
(indication d'unité de données UN)	Données d'utilisateur UN

Les primitives et les paramètres de service implicites sont équivalents à ceux définis dans la Rec. X.213 du CCITT | ISO 8348/AD1 (CLNS).

7.3 Attributs d'association de sécurité

Les attributs suivants commandent la mise en œuvre du protocole NLSP-CL. Leur description inclut la mnémonique utilisée pour se référer à ces attributs dans la présente Spécification.

NOTE – Lorsqu'un attribut SA est «imposé par l'ASSR», l'ASSR peut définir une seule valeur ou une série de valeurs. Lorsque l'ASSR définit une série de valeurs, la valeur d'attribut peut être établie par la gestion des systèmes OSI, par un échange de données de protocole SA-P ou par d'autres moyens qui sortent du cadre de la présente Spécification.

– Services de sécurité sélectionnés pour l'association SA:

DOAuth: Nombre entier compris entre des limites imposées par le niveau d'authentification d'origine des données de l'ASSR.

La valeur de cet attribut doit être fixée préalablement ou lors de l'établissement de l'association SA.

CLConf: Nombre entier compris entre des limites imposées par le niveau de confidentialité en mode sans connexion de l'ASSR.

La valeur de cet attribut doit être fixée préalablement ou lors de l'établissement de l'association SA.

CLInt: Nombre entier compris entre des limites imposées par le niveau d'intégrité en mode sans connexion de l'ASSR.

La valeur de cet attribut doit être fixée préalablement ou lors de l'établissement de l'association SA.

7.4 Vérifications

En de nombreux points dans les descriptions qui suivent, l'entité NLSP-CL vérifie que certaines conditions sont satisfaites. Sauf spécification contraire, chaque fois qu'une telle vérification échoue, l'entité NLSP-CL doit rejeter les données en cours de traitement. A titre facultatif, l'entité peut également archiver un rapport d'audit. Il incombe aux autorités locales de déterminer quels échecs doivent faire l'objet d'un rapport d'audit.

7.5 Etablissement d'association SA dans la bande

Une association SA peut être établie dans la bande à l'aide d'un protocole d'association de sécurité (SA-P). Un protocole SA-P est défini dans l'Annexe C de la présente Spécification.

NOTE – Actuellement, le protocole SA-P n'inclut aucune procédure de reprise et il faut donc veiller à ce que la fiabilité nécessaire soit assurée lorsqu'on utilise ce protocole avec le protocole NLSP-CL.

7.6 Traitement d'une demande NLSP-UNITDATA

7.6.1 Vérifications initiales et identification de l'association SA

A la réception d'une demande NLSP-UNITDATA, la NLSPE vérifie si les communications non protégées sont autorisées en fonction des exigences du service de sécurité local et de la paire adresse d'origine/adresse de destination. Si les communications non protégées sont autorisées, les paramètres de service NLSP sont copiés directement dans les paramètres de service UN équivalents d'une demande UN-UNITDATA et aucune autre action n'est entreprise par la NLSPE.

Si des communications protégées sont nécessaires, les vérifications initiales et l'identification des procédures SA décrites au 6.3 suivies des procédures indiquées ci-dessous doivent être mises en œuvre.

7.6.2 Protection de la primitive NLSP-UNITDATA

La NLSPE doit exécuter les «fonctions de création de SDT PDU» définies au 6.4.1.1 avec le champ type de données «NLSP-UNITDATA req/ind» contenant:

a) si l'attribut Param_Prot est VRAI, l'adresse NLSP d'origine;

b) si l'attribut Param_Prot est VRAI, l'adresse NLSP de destination;

c) le paramètre données d'utilisateur NLSP.

Le marqueur de champ complet/partiel («Last/Not last») doit être mis à «Last» (c'est-à-dire que le bit 7 du champ type de données est forcé à zéro).

7.6.3 Demande du réseau

La SDT PDU doit être transmise au protocole inférieur suivant sous la forme d'un paramètre données d'utilisateur UN d'une demande UN-UNITDATA.

Si l'attribut Param_Prot est VRAI, l'adresse UN d'origine doit être l'adresse UN de l'entité NLSP locale; sinon, l'adresse d'origine NLSP doit être copiée dans l'adresse d'origine UN.

Si l'attribut Param_Prot est VRAI, l'adresse de destination UN doit être l'adresse Peer_Adr; sinon, l'adresse de destination NLSP doit être copiée dans l'adresse de destination UN.

Le paramètre UN QOS doit être déterminé par la politique locale mais peut être copié à partir du paramètre NLSP QOS.

NOTE – Si les paramètres enregistrement de la voie d'acheminement et routage d'origine sont inclus dans les paramètres NLSP QOS et ne sont pas transmis sous la forme de paramètres QOS, la qualité de service QOS spécifiée peut ne pas être assurée pour la partie de la voie d'acheminement entre les entités NLSP-CL d'origine et de destination.

7.7 Traitement de l'indication UN-UNITDATA

7.7.1 Vérifications initiales et traitement

Si aucune SDT PDU n'est présente, la NLSPE vérifie si les communications non protégées sont autorisées en fonction des exigences du service de sécurité local et de la paire adresse d'origine/adresse de destination. Si les communications non protégées sont autorisées, les paramètres de service UN sont copiés directement dans les paramètres de service NLSP équivalents d'une demande NLSP-UNITDATA et aucune autre action n'est entreprise par la NLSPE. Si les communications non protégées ne sont pas autorisées, les procédures décrites au 7.4 sont mises en œuvre. Aucune autre action n'est entreprise par la NLSPE.

Si une SDT PDU est présente, la NLSPE doit identifier, parmi les associations SA dont elle dispose, une association SA avec un attribut My_SA-ID égal au champ SA-ID de la SDT PDU reçue. Toutes les autres opérations se réfèrent à cettte association SA identifiée.

La NLSPE doit exécuter les opérations de traitement communes définies au 6.4.2.1. En outre, les vérifications suivantes doivent être effectuées:

a) si le champ de type de données n'est «lié à aucune primitive de service NLSP», la SDT PDU doit cesser d'être traitée dans le cadre de ces procédures. Dans le cas contraire, il convient de vérifier que le champ de type de données est NLSP-UNITDATA;

NOTES

1 La valeur du marqueur de champ complet/partiel («Last/Not last») (c'est-à-dire le bit 7 du champ type de données) peut être ignorée.

2 La mise en œuvre de la fonction de remplissage de trafic ou d'échange de tests en mode sans connexion sort du cadre du protocole NLSP.

b) si l'attribut Param_Prot est VRAI, il convient de vérifier la SDT PDU pour s'assurer que les champs suivants sont présents:

1) adresse de destination;

2) adresse d'origine.

Une indication NLSP-UNITDATA doit être transmise à l'utilisateur NLSP avec paramètres réglés et adresse vérifiée comme indiqué au 7.7.2.

7.7.2 Paramètres de l'indication NLSP-CL

7.7.2.1 Paramètres d'adresse

Si l'attribut Param_Prot est VRAI, la NLSPE doit régler les paramètres de service aux valeurs contenues dans la SDT PDU.

Si l'attribut Param_Prot est FAUX, les valeurs doivent être extraites des paramètres d'indication UN comme suit:

a) adresse d'origine NLSP = adresse d'origine UN; et

b) adresse de destination NLSP = adresse de destination UN.

Il convient de vérifier que l'adresse de destination NLSP, réglée comme indiqué ci-dessus, est une adresse NLSP desservie par cette entité NLSP, conformément à la politique de sécurité locale.

Il convient de vérifier que l'adresse d'origine NLSP, réglée comme indiqué ci-dessus, est une adresse NLSP contenue dans l'attribut SA Adr_Served.

7.7.2.2 Paramètres QOS

Les paramètres QOS sont copiés du service UN dans le service NLSP.

7.7.2.3 Données d'utilisateur

Les données du champ de données d'utilisateur extraites du champ Octet-String-Before-Encapsulation de la SDT PDU doivent être transmises à l'utilisateur NLSP dans le paramètre NLSP Userdata de l'indication NLSP-UNITDATA.

8 Fonctions de protocole pour le protocole NLSP-CO

8.1 Services assurés par le protocole NLSP-CO

Les primitives des services assurés par le protocole NLSP-CO sont les suivantes:

Primitives	*Paramètres*
NLSP-CONNECT Request (demande de connexion NLSP) NLSP-CONNECT Indication (indication de connexion NLSP)	Adresse NLSP appelée Adresse NLSP appelante Sélection de confirmation de réception NLSP Sélection de données exprès NLSP Ensemble de paramètres NLSP QOS Données d'utilisateur NLSP
NLSP-CONNECT Response (réponse à une demande NLSP) NLSP-CONNECT Confirm (confirmation de connexion NLSP)	Adresse NLSP appelée Sélection de confirmation de réception NLSP Sélection de données exprès NLSP Ensemble de paramètres NLSP QOS Données d'utilisateur NLSP
NLSP-DATA Request (demande de données NLSP) NLSP-DATA Indication (indication de données NLSP)	Données d'utilisateur NLSP Demande de confirmation NLSP
NLSP-DATA-ACKNOWLEDGE Request (demande d'accusé de réception de données NLSP) NLSP-DATA-ACKNOWLEDGE Indication (indication d'accusé de réception de données NLSP)	
NLSP-EXPEDITED-DATA Request (demande de données exprès NLSP) NLSP-EXPEDITED-DATA Indication (indication de données exprès NLSP)	Données d'utilisateur NLSP
NLSP-RESET Request (demande de réinitialisation NLSP) NLSP-RESET Indication (indication de réinitialisation NLSP)	Raison NLSP Entité appelante NLSP Raison NLSP
NLSP-RESET Response (réponse à une demande de réinitialisation NLSP) NLSP-RESET Confirmation (confirmation de réinitialisation NLSP)	
NLSP-DISCONNECT Request (demande de déconnexion NLSP) NLSP-DISCONNECT Indication (indication de déconnexion NLSP)	Entité appelante NLSP Raison NLSP Données d'utilisateur NLSP Adresse NLSP appelée

NOTE – Le paramètre entité appelante ne s'applique pas à la primitive de demande.

Les primitives et les paramètres de service sont directement équivalents à ceux définis dans la Rec. X.213 du CCITT | ISO 8348.

8.2 Services implicites

Les services assurés implicitement par le protocole NLSP à sa limite inférieure seront désignés par le préfixe «UN» (pour «réseau de base»); il s'agit d'une interface notionnelle (voir 5.1).

L'interface UN est modélisée en deux parties:

a) une définition des primitives et des paramètres de service UN (voir ci-dessous);

b) une mise en correspondance du service UN (voir 5.1) avec un service de réseau normalisé ou directement avec la Rec. X.25 du CCITT | ISO 8208.

Les Annexes A et B définissent la mise en correspondance de l'interface de service notionnelle avec le service de réseau et la Rec. X.25 ou ISO 8208.

Les primitives UN implicites pour le protocole NLSP-CO sont les suivantes:

Primitives	*Paramètres*
UN-CONNECT Request (demande de connexion UN) UN-CONNECT Indication (indication de connexion UN)	Adresse UN appelée Adresse UN appelante Sélection de confirmation de réception UN Sélection de données exprès UN Ensemble de paramètres UN QOS Données d'utilisateur UN Authentification UN[1)]
UN-CONNECT Response (réponse à une demande de connexion UN) UN-CONNECT Confirm (confirmation de connexion UN)	Adresse UN appelée Sélection de confirmation de réception UN Sélection de données exprès UN Ensemble de paramètres UN QOS Données d'utilisateur UN Authentification UN[1)]
UN-DATA Request (demande de données UN) UN-DATA Indication (indication de données UN)	Données d'utilisateur UN Demande de confirmation UN
UN-DATA-ACKNOWLEDGE Request (demande d'accusé de réception de données UN) UN-DATA-ACKNOWLEDGE Indication (indication d'accusé de réception de données UN)	
UN-EXPEDITED-DATA Request (demande de données exprès UN) UN-EXPEDITED-DATA Indication (indication de données exprès UN)	Données d'utilisateur UN
UN-RESET Request (demande de réinitialisation UN) UN-RESET Indication (indication de réinitialisation UN)	Raison UN Entité UN appelante Raison UN
UN-RESET Response (réponse à une demande de réinitialisation UN) UN-RESET Confirm (confirmation de réinitialisation UN)	

1) Le paramètre d'authentification UN est utilisé pour acheminer la CSC PDU, ce qui permet un codage efficace lorsque le protocole NLSP est mis en œuvre conformément à la Rec. X.25 ou ISO 8208 où le paramètre d'authentification UN peut être acheminé par le champ de service complémentaire de protection d'ETTD (voir l'Annexe B).

UN-DISCONNECT Request (demande de déconnexion UN)	Raison UN Données d'utilisateur UN Adresse UN appelée
UN-DISCONNECT Indication (indication de déconnexion UN)	Entité UN appelante Raison UN Données d'utilisateur UN Adresse UN appelée

Les Annexes A et B définissent la mise en correspondance de l'authentification UN avec la Rec. X.213 du CCITT | ISO 8348 et avec la Rec. X.25 ou ISO 8208.

NOTE – Lorsque le protocole NLSP est utilisé en étroite association avec la Rec. X.25 du CCITT | ISO 8208, il peut utiliser d'autres codages qui tirent pleinement parti du protocole sous-jacent alors que la variante de mise en correspondance avec la Rec. X.213 du CCITT | ISO 8348 implique uniquement l'utilisation d'un service de réseau de base.

8.3 Attributs d'association de sécurité

Les attributs suivants commandent la mise en œuvre du protocole NLSP-CO. Leur description inclut la mnémonique utilisée pour se référer à ces attributs dans la présente Spécification.

NOTE 1 – Lorsqu'un attribut SA est «imposé par l'ASSR», l'ASSR peut définir une seule valeur ou une série de valeurs. Lorsque l'ASSR définit une série de valeurs, la valeur d'attribut peut être établie par la gestion des systèmes OSI, par un échange de données de protocole SA-P ou par d'autres moyens qui sortent du cadre de la présente Spécification.

a) *Services de sécurité sélectionnés pour l'association SA:*

PE Auth: Nombre entier compris entre des limites imposées par le niveau d'authentification d'entité homologue de l'ASSR.

CO Conf: Nombre entier compris entre des limites imposées par le niveau de confidentialité en mode connexion de l'ASSR.

CO Int: Nombre entier compris entre des limites imposées par l'intégrité en mode connexion sans reprise de l'ASSR.

La valeur de ces attributs doit être fixée préalablement ou lors de l'établissement de l'association SA.

b) *Attributs liés au protocole CO:*

Retain_On_Disconnect: Valeur booléenne

Indique si les attributs SA doivent être conservés lors de la déconnexion.

La valeur de cet attribut doit être fixée lors de l'établissement de l'association SA ou préalablement.

Protect_Connect_Params: Valeur booléenne

Protection des données d'utilisateur NLSP dans les primitives NLSP-CONNECT et NLSP-DISCONNECT ainsi que d'autres paramètres de service dans les primitives NLSP-CONNECT et NLSP-DISCONNECT si l'attribut Param_Prot est également VRAI.

La valeur de cet attribut doit être imposée par l'ASSR.

NOTE 2 – L'attribut Param_Prot ne peut être VRAI si l'attribut Protect_Connect_Params est FAUX.

No_Header: Valeur booléenne

La protection fondée sur l'attribut No_Header, si celui-ci est vrai, doit être utilisée pour protéger les données (par exemple, à l'aide des procédures définies à l'article 12).

La valeur de cet attribut doit être imposée par l'ASSR.

8.4 Vérifications et autres fonctions communes

En de nombreux points dans les descriptions qui suivent, il est indiqué que certaines conditions doivent être satisfaites. Sauf spécification contraire, chaque fois qu'une vérification échoue au cours des procédures NLSP-CONNECT ou NLSP-DISCONNECT, une demande UN-DISCONNECT et une indication NLSP-DISCONNECT doivent être émises

en conséquence. Si un tel événement se produit après l'établissement de la connexion, la NLSPE doit rejeter les données en cours de traitement et doit, en fonction d'une décision prise localement, invoquer:

- soit une procédure UN-RESET déclenchée par le NLSP, comme indiqué au 8.8.5;
- soit une demande UN-DISCONNECT et une indication NLSP-DISCONNECT.

A titre facultatif, l'entité peut également archiver un rapport d'audit. Il incombe aux autorités locales de décider quelles informations d'audit doivent être enregistrées.

De même, une séquence d'événements prévue est indiquée dans les procédures décrites ci-dessous. Si cette séquence n'est pas suivie, un événement imprévu doit être traité de la même manière qu'un échec de vérification.

Lorsque les descriptions qui suivent se réfèrent à la création ou à la vérification de CSC PDU ou de PDU de transfert de données sûres, des procédures appropriées spécifiques des mécanismes, par exemple, celles décrites aux articles 9 à 12 de la présente Spécification, doivent être appliquées.

8.5 Fonctions NLSP-CONNECT

8.5.1 Procédures initiales

8.5.1.1 Vérifications initiales – Demande NLSP-CONNECT

A la réception d'une demande NLSP-CONNECT, la NLSPE doit vérifier si les communications non protégées sont autorisées en fonction des exigences du service de sécurité local et de la paire adresse appelante/adresse appelée. Si les communications non protégées sont autorisées, les paramètres de service NLSP et UN sont copiés directement dans les paramètres de service UN et NLSP équivalents pour toutes les primitives de service NLSP et UN ultérieures jusqu'après la réception d'une indication UN-DISCONNECT. Aucune autre action n'est entreprise par la NLSPE pendant la durée de la connexion.

Si des communications protégées sont nécessaires, la NLSPE doit suivre les procédures applicables aux vérifications initiales et à l'identification de l'association de sécurité décrites respectivement aux 6.3.1 et 6.3.2 puis appliquer les procédures définies aux 8.5.2, 8.5.3 ou 8.5.4. Les procédures appropriées dépendent du mode d'établissement de la connexion sélectionné comme indiqué au 8.5.1.2. Le même paragraphe est alors utilisé pour les primitives de service UN-CONNECT et NLSP-CONNECT ultérieures sur cette connexion UN.

8.5.1.2 Mode d'établissement de connexion NLSP

S'il existe actuellement une association SA avec les caractéristiques requises, celle-ci peut être utilisée pour protéger la connexion. Dans le cas contraire, une nouvelle association SA est établie dans la bande au titre des fonctions NLSP-CONNECT ou hors bande dans un délai donné. Si ni l'une ni l'autre de ces fonctions ne peut être exécutée, une primitive NLSP-DISCONNECT doit être renvoyée.

Il existe deux modes fondamentaux d'établissement d'une connexion NLSP, avec des variantes permettant l'établissement de l'association SA dans la bande comme suit:

a) **paramètres NLSP-CONNECT dans les paramètres UN-CONNECT**; variante dans laquelle les données de protocole pour assurer l'authentification et les paramètres NLSP-CONNECT sont échangés dans les paramètres UN-CONNECT;

b) **paramètres NLSP-CONNECT dans les paramètres UN-CONNECT avec SA-P**; variante dans laquelle l'établissement de l'association SA dans la bande est effectué dans une primitive UN-DATA sur une connexion préalable avant l'établissement d'une seconde connexion UN avec acheminement des paramètres d'authentification et NLSP-CONNECT dans les paramètres UN-CONNECT, comme en a) ci-dessus;

c) **paramètres NLSP-CONNECT dans les paramètres UN-DATA**; variante dans laquelle un échange de données d'authentification est effectué dans les paramètres UN-CONNECT et est suivi d'un échange de paramètres NLSP-CONNECT dans les paramètres UN-DATA;

d) **paramètres NLSP-CONNECT dans les paramètres UN-DATA avec SA-P**; variante dans laquelle un échange de données de protocole SA-P est effectué dans les paramètres UN-DATA et est suivi d'un échange de paramètres NLSP-CONNECT dans les paramètres UN-DATA.

Le choix du mode le plus approprié relève d'une décision qui doit être prise au niveau local par la NLSPE appelante en fonction des conditions existantes (ou des conditions prévues) d'établissement de connexion NLSP et de l'environnement dans lequel le protocole NLSP est mis en œuvre.

Le choix d'un protocole SA-P est indiqué par le marqueur SA-P dans la CSC PDU. Le choix de la variante paramètres NLSP-CONNECT dans les paramètres UN-CONNECT ou paramètres NLSP-CONNECT dans les paramètres UN-DATA est indiqué à la NLSPE distante par le marqueur UNC-UND (voir le Tableau 8-2).

Dans les deux derniers modes (paramètres NLSP-CONNECT dans les paramètres UN-DATA avec ou sans protocole SA-P), les paramètres NLSP-CONNECT sont codés dans une SDT PDU et ces modes ne peuvent donc être utilisés dans le mode No_Header.

Dans les deux premiers modes (paramètres NLSP-CONNECT dans les paramètres UN-CONNECT avec ou sans protocole SA-P), les paramètres NLSP-CONNECT seront protégés dans une SDT PDU si l'attribut No_Header est FAUX et si l'attribut Protect_Connect_Params est VRAI. Cependant, ces modes ne peuvent être utilisés si la SDT PDU qui en résulte est plus longue que l'espace disponible dans les données d'utilisateur UN de la primitive UN-CONNECT.

Le Tableau 8-1 indique les restrictions qui s'appliquent aux divers modes d'établissement de connexion définis ci-dessus. Ce tableau peut être utilisé pour déterminer quelles procédures d'établissement de l'appel conviennent à un profil donné.

Tableau 8-1 – Tableau indiquant les restrictions applicables au mode d'établissement de connexion NLSP

SA-P	No_Header	Protect_ Connect_ Params	Limites de longueur de SDT PDU (voir Notes ci-dessous)	Mode	Procédures d'établissement de connexion
VRAI	VRAI	VRAI ou FAUX		NLSP-CONNECT dans UN-CONNECT avec SA-P	8.5.3 puis 8.5.2.2 à 8.5.2.4
VRAI	FAUX	VRAI	SDT < = max UN Userdata	NLSP-CONNECT dans UN-CONNECT avec SA-P	8.5.3 puis 8.5.2.2 à 8.5.2.4
VRAI	FAUX	FAUX		NLSP-CONNECT dans UN-CONNECT avec SA-P	8.5.3 puis 8.5.2.2 à 8.5.2.4
VRAI	FAUX	VRAI ou FAUX		NLSP-CONNECT dans UN-DATA avec SA-P	8.5.4
FAUX	VRAI	VRAI ou FAUX		NLSP-CONNECT dans UN-CONNECT	8.5.2
FAUX	FAUX	VRAI	SDT < = max UN Userdata	NLSP-CONNECT dans UN-CONNECT	8.5.2
FAUX	FAUX	FAUX		NLSP-CONNECT dans UN-CONNECT	8.5.2
FAUX	FAUX	VRAI ou FAUX		NLSP-CONNECT dans UN-DATA	8.5.4

NOTES

1 Le sigle SDT désigne la longueur maximale possible de la SDT PDU qui peut être créée pendant l'établissement de la connexion pour l'environnement dans lequel le protocole NLSP est mis en œuvre.

2 On admet implicitement que les limites qui s'appliquent à la longueur des données d'utilisateur UN (UN Userdata) s'appliquent également à la longueur des données d'utilisateur NLSP (NLSP Userdata).

3 Pour la mise en correspondance UN avec la Rec. X.213 du CCITT | ISO 8348, la longueur «max UN Userdata» (données d'utilisateur UN max) est la longueur maximale de données d'utilisateur qui peut être acheminée dans les primitives de service N-CONNECT du service de réseau (par exemple, 128 pour la Rec. X.223 du CCITT | ISO 8878 et la Rec. X.25 | ISO 8208) moins la longueur de l'unité CSC PDU.

4 Pour la mise en correspondance UN directement avec la Rec. X.25 | ISO 8208, la longueur «max UN Userdata» est 128.

8.5.1.3 Vérifications initiales – Indication UN-CONNECT

A la réception d'une indication UN-CONNECT sans la présence d'une CSC PDU dans le paramètre d'authentification UN, la NLSPE doit vérifier si les communications non protégées sont autorisées en fonction des exigences du service de sécurité local et de la paire adresse appelante/adresse appelée. Si les communications non protégées sont autorisées, les paramètres de service NLSP et UN sont copiés directement dans les paramètres de service UN et NLSP équivalents pour toutes les primitives de service NLSP et UN ultérieures jusqu'après la réception d'une indication UN-DISCONNECT. Aucune autre action n'est entreprise par la NLSPE pendant la durée de la connexion.

Si les communications non protégées ne sont pas autorisées et si aucune CSC PDU n'est présente, les procédures définies au 8.4 pour l'échec de vérification sont mises en œuvre.

Si une CSC PDU est présente, les procédures définies aux 8.5.2, 8.5.3 ou 8.5.4 sont exécutées selon la valeur des marqueurs SA-P et UNC-UND dans le champ de type de PDU, comme indiqué dans le Tableau 8-2. S'il est positionné, le marqueur SA-P indique que des échanges de données de protocole SA-P dans la bande doivent être effectués par le protocole NLSP. S'il est positionné, le marqueur UNC-UND indique que les paramètres NLSP-CONNECT doivent être acheminés dans une primitive UN-DATA au lieu de UN-CONNECT. Le même paragraphe est alors utilisé pour les primitives de service UN-CONNECT et NLSP-CONNECT ultérieures sur cette connexion UN.

Tableau 8-2 – Marqueurs de CSC PDU identifiant les procédures d'établissement de connexion NLSP

Marqueur UNC-UND	Marqueur SA-P	Procédures d'établissement de connexion NLSP
Positionné	Positionné	8.5.4 (NLSP-CONNECT dans UN-DATA)
Positionné	Libre	8.5.4 (NLSP-CONNECT dans UN-DATA)
Libre	Positionné	8.5.3 (NLSP-CONNECT dans UN-CONNECT avec SA-P)
Libre	Libre	8.5.2 (NLSP-CONNECT dans UN-CONNECT)

8.5.2 Paramètres NLSP-CONNECT dans les paramètres UN-CONNECT

La séquence d'événements prévue pour l'établissement de connexion NLSP avec les paramètres NLSP-CONNECT dans les paramètres UN-CONNECT est illustrée sur la Figure 8-1.

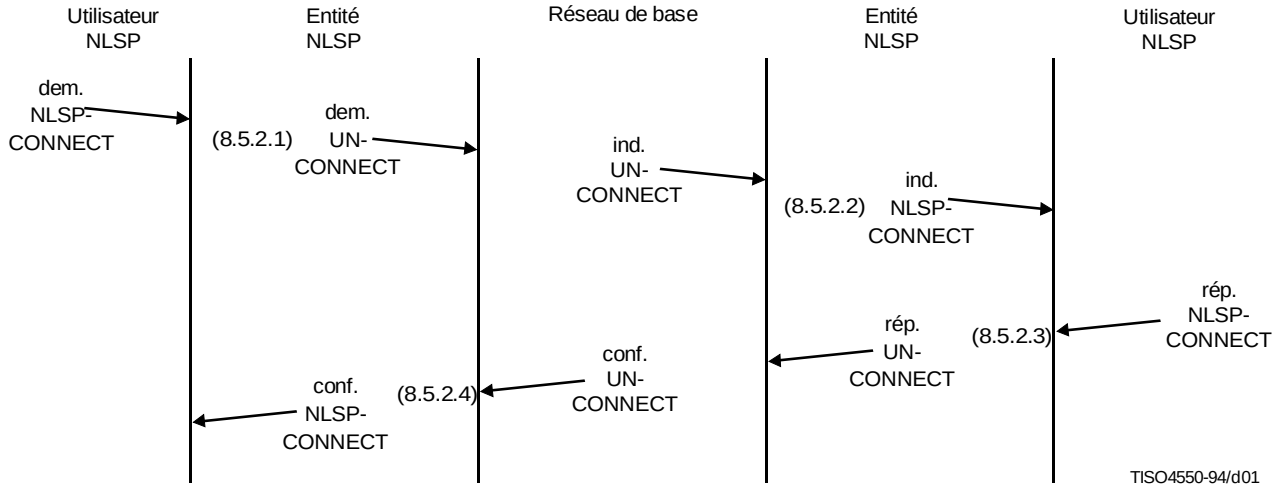


Figure 8-1 – Chronogramme de primitives de service pour les paramètres NLSP-CONNECT dans les paramètres UN-CONNECT

8.5.2.1 Demande NLSP-CONNECT

Lors d'une demande NLSP-CONNECT, si les paramètres NLSP-CONNECT doivent être acheminés dans les paramètres UN-CONNECT, les procédures suivantes doivent être mises en œuvre:

a) si l'attribut Protect_Connect_Params est VRAI et si l'attribut No_Header est VRAI, tout paramètre NLSP Userdata doit être encapsulé comme indiqué au 6.4.1.2. Ce paramètre est placé dans le paramètre UN Userdata;

b) si l'attribut Protect_Connect_Params est VRAI, si l'attribut No_Header est FAUX et si l'attribut Param_Prot est VRAI, une SDT PDU contenant l'adresse NLSP appelée, l'adresse NLSP appelante et le paramètre NLSP Userdata, est créée comme indiqué au 6.4.1.1, avec type de données «dem./ind. NLSP-CONNECT». Cette PDU est placée dans le paramètre UN Userdata;

c) si l'attribut Protect_Connect_Params est VRAI, si l'attribut No_Header est FAUX et si l'attribut Param_Prot est FAUX, une SDT PDU contenant le paramètre NLSP Userdata, s'il est présent, est émise, comme indiqué au 6.4.1.1, avec type de données «dem./ind. NLSP-CONNECT». Cette PDU est placée dans le paramètre UN Userdata;

d) si l'attribut Protect_Connect_Params est FAUX, le paramètre NLSP Userdata est placé dans le paramètre UN Userdata;

e) une CSC PDU est préparée avec:

   1) marqueur UNC-UND libre;

   2) identificateur SA-ID de l'association SA applicable placé dans le champ SA-ID;

   3) marqueur SA-P libre;

   4) contenu de CSC réglé selon le premier échange de CSC conformément aux procédures spécifiques des mécanismes telles que celles décrites au 10.3;

f) une demande UN-CONNECT doit être invoquée avec:

   1) si l'attribut Param_Prot est présent, adresse UN appelée réglée à la valeur Peer_Adr, sinon NLSP Called Address (adresse NLSP appelée);

   2) si l'attribut Param_Prot est présent, adresse UN appelante réglée à la valeur local NLSPE UN-address (adresse UN de NLSPE locale), sinon NLSP Calling Address (adresse NLSP appelante);

   3) sélection de confirmation de réception et sélection de données exprès UN réglées aux valeurs déterminées localement à partir de la sélection de confirmation de réception et de la sélection de données exprès NLSP;

   4) paramètre UN QOS réglé à une valeur déterminée localement à partir du paramètre NLSP QOS;

   5) paramètre UN Userdata réglé comme indiqué aux points a) à d) ci-dessus;

   6) paramètre d'authentification UN réglé selon la CSC PDU comme indiqué en e) ci-dessus;

g) la NLSPE appelante attend une confirmation UN-CONNECT comme indiqué au 8.5.2.4 ou une indication UN-DISCONNECT comme indiqué au 8.10.

8.5.2.2 Indication UN-CONNECT – UNC-UND libre et SA-P libre

A la réception d'une indication UN-CONNECT avec authentification UN contenant une CSC PDU avec marqueur UNC-UND libre et marqueur SA-P libre:

a) la NLSPE doit identifier, parmi les associations SA dont elle dispose, une association SA avec attribut My_SA-ID égal au champ SA-ID de la CSC PDU reçue. Toutes les autres opérations se réfèrent à cette association SA identifiée;

b) le contenu de la CSC PDU doit être vérifié conformément aux procédures spécifiques des mécanismes telles que celles décrites au 10.3. Le contenu de la CSC PDU renvoyée en guise de réponse doit être conservé pour utilisation lors du traitement de la réponse NLSP-CONNECT comme indiqué au 8.5.2.3;

c) si l'attribut Protect_Connect_Params est VRAI et si l'attribut No_Header est VRAI, tout paramètre UN Userdata doit être décapsulé comme indiqué au 6.4.2.2. Ce paramètre est placé dans le paramètre NLSP Userdata. Les autres paramètres d'indication NLSP-CONNECT sont copiés à partir des paramètres d'indication UN-CONNECT;

d) si l'attribut Protect_Connect_Params est VRAI, si l'attribut No_Header est FAUX et si le paramètre Param_Prot est VRAI, la SDT PDU dans le paramètre UN Userdata est vérifiée comme indiqué au 6.4.2.1. Il convient de vérifier que le champ de type de données est dem./ind. NLSP-CONNECT. Les champs de contenu adresse NLSP appelée, adresse NLSP appelante et données d'utilisateur NLSP de la SDT PDU doivent être placés dans les paramètres d'indication NLSP-CONNECT. Les paramètres sélection de confirmation de réception et sélection de données exprès UN ainsi que l'ensemble de paramètres UN QOS doivent être copiés dans les paramètres d'indication NLSP-CONNECT équivalents;

e) si l'attribut Protect_Connect_Params est VRAI, si l'attribut No_Header est FAUX et si l'attribut Param_Prot est FAUX, la SDT PDU du paramètre UN Userdata est vérifiée, si elle est présente, comme indiqué au 6.4.2.1. Il convient de vérifier que le champ de type de données est dem./ind. NLSP-CONNECT. Le champ de contenu données d'utilisateur de la SDT PDU doit être placé dans le paramètre NLSP Userdata. Les autres paramètres d'indication NLSP-CONNECT sont copiés à partir des paramètres d'indication UN-CONNECT;

f) si l'attribut Protect_Connect_Params est FAUX, tous les paramètres d'indication UN-CONNECT sont copiés dans les paramètres d'indication NLSP-CONNECT;

g) il convient de vérifier que l'adresse NLSP appelée, réglée comme indiqué ci-dessus, est une adresse NLSP desservie par cette entité NLSP selon les décisions prises localement;

h) il convient de vérifier que l'adresse NLSP appelante, réglée comme indiqué ci-dessus, est une adresse NLSP dans l'attribut SA Adr_Served;

i) si une étiquette de sécurité est établie pour la connexion, cette étiquette doit être vérifiée en fonction de l'ensemble d'étiquettes autorisées dans l'attribut SA Label_Set;

j) l'indication NLSP-CONNECT doit être transmise à l'utilisateur NLSP;

NOTE – L'ensemble de paramètres sélection de confirmation de réception et sélection de données exprès NLSP ainsi que NLSP QOS peut être modifié de manière à prendre une valeur déterminée localement avant d'être transmis à l'utilisateur NLSP.

k) la NLSPE appelée attend une réponse NLSP-CONNECT comme indiqué au 8.5.2.3 ou une demande NLSP-DISCONNECT ou une indication UN-DISCONNECT comme indiqué au 8.10.

8.5.2.3 Réponse NLSP-CONNECT

A la réception d'une réponse NLSP-CONNECT:

a) si l'attribut Protect_Connect_Params est VRAI et si l'attribut No_Header est VRAI, tout paramètre NLSP Userdata doit être encapsulé comme indiqué au 6.4.1.2. Ce paramètre est placé dans le paramètre UN Userdata;

b) si l'attribut Protect_Connect_Params est VRAI, si l'attribut No_Header est FAUX et si l'attribut Param_Prot est VRAI, une SDT PDU contenant l'adresse NLSP appelée et le paramètre NLSP Userdata est émise comme indiqué au 6.4.1.1 avec type de données rép./conf. NLSP-CONNECT. Cette unité est placée dans le paramètre UN Userdata;

c) si l'attribut Protect_Connect_Params est VRAI, si l'attribut No_Header est FAUX, si l'attribut Param_Prot est FAUX et si le paramètre NLSP Userdata est présent, une SDT PDU contenant le paramètre NLSP Userdata est émise, comme indiqué au 6.4.1.1, avec type de données rép./conf. NLSP-CONNECT. Cette unité est placée dans le paramètre UN Userdata;

d) si l'attribut Protect_Connect_Params est FAUX, le paramètre NLSP Userdata est placé dans le paramètre UN Userdata;

e) s'il n'est pas possible d'intégrer les données engendrées aux points a) à d) ci-dessus dans le paramètre UN Userdata, ces procédures doivent être abandonnées, comme indiqué au 8.4;

f) une CSC PDU doit être créée avec:

1) marqueurs SA-P et UNC-UND libres;

2) identificateur SA-ID réglé à la valeur de l'identificateur SA-ID de la CSC PDU reçue dans l'indication UN-CONNECT;

3) contenu de CSC réglé à la valeur renvoyée à la suite de la précédente invocation des procédures spécifiques des mécanismes au 8.5.2.2 b);

g) une réponse UN-CONNECT doit être envoyée avec:

1) si l'attribut Param_Prot est VRAI, paramètre adresse UN appelée réglé à la valeur adresse UN de l'entité NLSP locale, sinon à la valeur du paramètre adresse NLSP appelée;

2) paramètres sélection de confirmation de réception et sélection de données exprès UN réglés aux valeurs déterminées localement à partir des paramètres confirmation de sélection de réception et sélection de données exprès NLSP;

3) paramètre UN QOS réglé aux valeurs déterminées localement à partir du paramètre NLSP QOS;

4) paramètre UN Userdata réglé comme indiqué aux points a) à d) ci-dessus;

5) paramètre UN authentification réglé à la valeur de la CSC PDU, comme indiqué en g) ci-dessus;

h) si cela est nécessaire au titre des procédures spécifiques des mécanismes d'authentification et d'échange de CSC (telles que celles décrites au 10.3), la NLSPE appelée peut attendre une SDT PDU dans le paramètre UN-DATA avant de terminer l'établissement de la connexion NLSP et de traiter les primitives NLSP-DATA reçues de l'utilisateur NLSP. Dans le cas contraire, la NLSPE appelée a maintenant terminé ses procédures d'établissement de connexion NLSP et peut entrer dans la phase de transfert de données.

NOTE – Si le mécanisme d'échange de CSC exige l'échange de plus de deux CSC PDU, celles-ci sont échangées dans une primitive UN-DATA avant la fin de l'établissement de la connexion.

8.5.2.4 Confirmation UN-CONNECT – UNC-UND libre et SA-P libre

A la réception d'une confirmation UN-CONNECT avec authentification UN contenant une CSC PDU avec marqueurs UNC-UND et SA-P libres:

a) le contenu de la CSC PDU est vérifié à l'aide des procédures spécifiques des mécanismes telles que celles décrites au 10.3;

b) si l'attribut Protect_Connect_Params est VRAI et si l'attribut No_Header est VRAI, tout paramètre UN Userdata doit être décapsulé comme indiqué au 6.4.2.2. Ce paramètre est placé dans le paramètre NLSP Userdata. Les autres paramètres de confirmation NLSP-CONNECT sont copiés à partir des paramètres de confirmation UN-CONNECT;

c) si l'attribut Protect_Connect_Params est VRAI, si l'attribut No_Header est FAUX et si l'attribut Param_Prot est VRAI, la SDT PDU dans le paramètre UN Userdata est vérifiée comme indiqué au 6.4.2.1. Il convient de vérifier que le champ de type de données est rép./conf. NLSP-CONNECT. Les champs de contenu adresse NLSP appelée et données d'utilisateur NLSP de la SDT PDU doivent être placés dans les paramètres de confirmation NLSP-CONNECT. Les paramètres de sélection de confirmation de réception et de sélection de données exprès UN ainsi que l'ensemble de paramètres UN QOS doivent être copiés dans les paramètres de confirmation NLSP-CONNECT;

d) si l'attribut Protect_Connect_Params est VRAI, si l'attribut No_Header est FAUX et si l'attribut Param_Prot est FAUX, la SDT PDU du paramètre UN Userdata, si elle est présente, est vérifiée comme indiqué au 6.4.2.1. Il convient de vérifier que le champ de type de données est rép./conf. NLSP-CONNECT. Le champ de contenu de données d'utilisateur de la SDT PDU doit être placé dans le paramètre NLSP Userdata. Les autres paramètres de confirmation NLSP-CONNECT doivent être copiés à partir des paramètres de confirmation UN-CONNECT;

e) si l'attribut Protect_Connect_Params est FAUX, tous les paramètres de confirmation UN-CONNECT doivent être copiés dans les paramètres de confirmation NLSP-CONNECT;

f) si elle est présente, l'adresse NLSP appelée doit être vérifiée en fonction d'une adresse NLSP contenue dans l'attribut SA Adr_Served;

g) la confirmation NLSP-CONNECT doit être transmise à l'utilisateur NLSP;

h) si cela est nécessaire au titre des procédures spécifiques des mécanismes d'authentification et d'échange de CSC (telles que celles décrites au 10.3), une SDT PDU peut être créée comme indiqué au 6.4.1.1 avec type de données n'étant «lié à aucune primitive de service NLSP» et ne contenant aucun champ de contenu autres que ceux nécessaires au titre de l'article 6. Cette unité doit être envoyée dans le paramètre UN Userdata d'une primitive UN-DATA.

NOTE – Si le mécanisme d'échange de CSC exige l'échange de plus de deux CSC PDU, celles-ci sont échangées dans une primitive UN-DATA avant la fin de l'établissement de la connexion.

Les procédures d'établissement de connexion NLSP sont maintenant terminées.

8.5.3 Paramètres NLSP-CONNECT dans les paramètres UN-CONNECT avec SA-P

La séquence d'événements prévue est illustrée sur la Figure 8-2.

8.5.3.1 Demande NLSP-CONNECT

Lors d'une demande NLSP-CONNECT, si les paramètres NLSP-CONNECT doivent être acheminés dans les paramètres UN-CONNECT et si l'établisement d'une association SA dans la bande est sélectionné, les procédures suivantes doivent être mises en œuvre:

a) une CSC PDU doit être préparée avec:
   1) marqueur UNC-UND libre;
   2) marqueur SA-P positionné et identificateur SA-ID, longueur de contenu et contenu de CSC PDU non présents;

b) une demande UN-CONNECT doit être envoyée avec:
   1) paramètre adresse UN appelée réglé à la valeur Peer_Adr;
   2) paramètre adresse UN appelante réglé à la valeur adresse UN d'entité NLSP locale;
   3) paramètre sélection de confirmation de réception UN réglé à une valeur déterminée localement;
   4) paramètre sélection de données exprès UN réglé à une valeur déterminée localement;
   5) paramètre UN QOS réglé à une valeur déterminée localement;
   6) données d'utilisateur UN vides;
   7) paramètre UN authentification réglé à la valeur de la CSC PDU;

c) la NLSPE appelante doit attendre une confirmation UN-CONNECT comme indiqué au 8.5.3.3 ou une indication UN-DISCONNECT comme indiqué au 8.10.

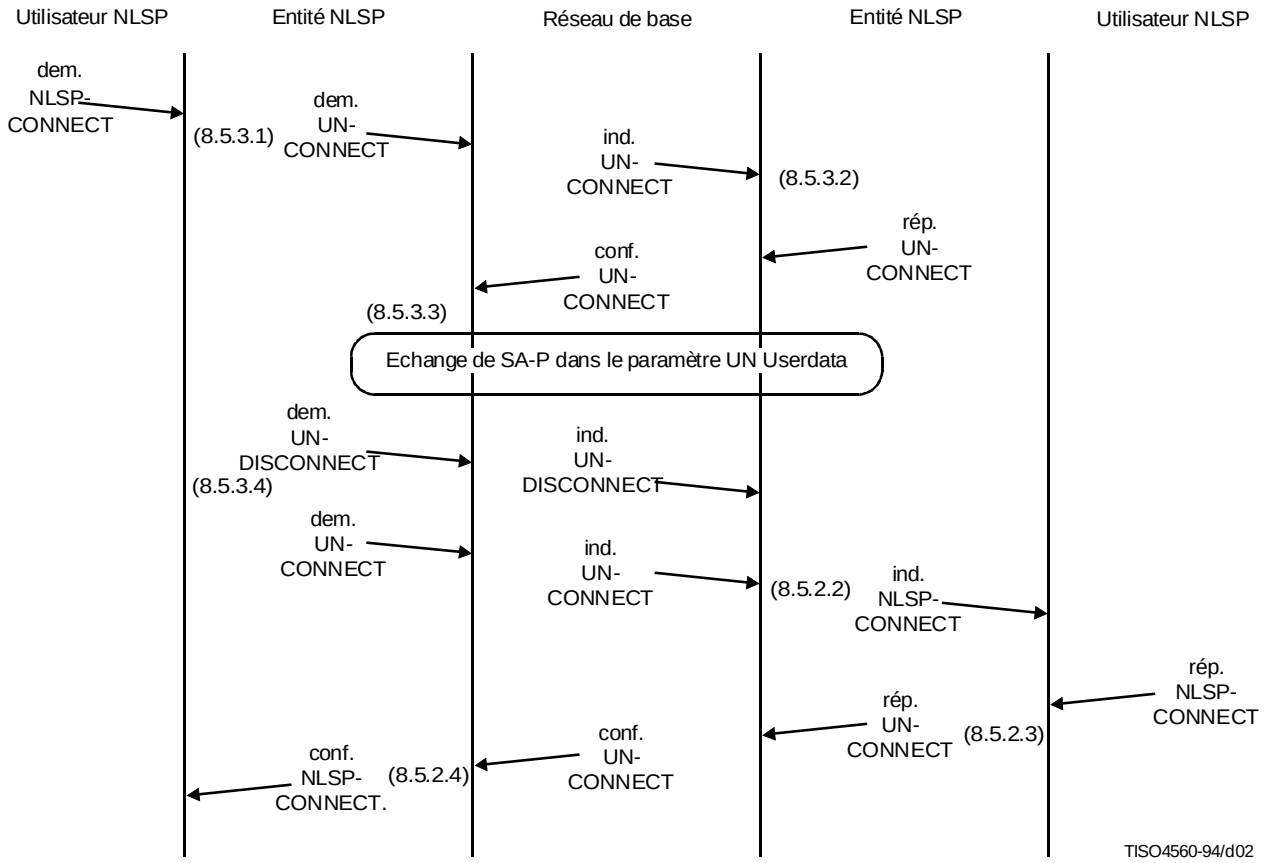


Figure 8-2 – Chronogramme de primitives de service pour les paramètres NLSP-CONNECT dans les paramètres UN-CONNECT avec SA-P

8.5.3.2 Indication UN-CONNECT – UNC-UND libre et SA-P positionné

A la réception d'une indication UN-CONNECT avec paramètre UN authentification contenant une CSC PDU avec marqueur UNC-UND libre et marqueur SA-P positionné:

a) le NLSP doit préparer une CSC PDU avec:

1) marqueur UNC-UND libre;

2) marqueur SA-P positionné;

3) contenu de CSC vide;

b) la NLSPE doit alors répondre à l'aide d'une réponse UN-CONNECT avec:

1) paramètre adresse UN appelée réglé à la valeur du paramètre adresse UN locale;

2) paramètres sélection de confirmation de réception et sélection de données exprès UN réglés à des valeurs déterminées localement à partir des paramètres contenus dans l'indication UN-CONNECT;

3) paramètre UN QOS réglé à une valeur déterminée localement à partir du paramètre UN QOS de l'indication UN-CONNECT;

4) données d'utilisateur UN vides;

5) paramètre UN Authentification réglé à la valeur de la CSC PDU.

La NLSPE appelée doit attendre un échange de données de protocole SA-P ou une indication UN-DISCONNECT comme indiqué au 8.10. Toute erreur dans le protocole SA-P doit être traitée comme une erreur conformément au 8.4.

8.5.3.3 Confirmation UN-CONNECT – UNC-UND libre et SA-P positionné

A la réception d'une confirmation UN-CONNECT avec paramètre UN authentification contenant une CSC PDU de réponse avec marqueur UNC-UND libre et marqueur SA-P positionné:

a) le protocole SA-P dans la bande doit être mis en œuvre;

b) la NLSPE appelante attend la fin de la mise en œuvre du protocole SA-P comme indiqué au 8.5.3.4 ou un paramètre UN-DISCONNECT comme indiqué au 8.10.

8.5.3.4 Fin de la mise en œuvre du protocole SA-P

A la fin de la mise en œuvre du protocole SA-P comme indiqué au 8.5.3.3, la NLSPE appelante doit appliquer les procédures suivantes:

a) une demande UN-DISCONNECT doit être envoyée par la NLSPE appelante avec raison réglée à la valeur «disconnect-normal-condition»; cette demande doit être suivie d'une demande UN-CONNECT avec paramètres de service réglés comme suit;

b) si l'attribut Protect_Connect_Params est VRAI et si l'attribut No_Header est VRAI, tout paramètre NLSP Userdata doit être encapsulé comme indiqué au 6.4.1.2. Ce paramètre est placé dans le paramètre UN Userdata;

c) si l'attribut Protect_Connect_Params est VRAI, si l'attribut No_Header est FAUX et si l'attribut Param_Prot est VRAI, une SDT PDU contenant les paramètres adresse NLSP appelée, adresse NLSP appelante et données d'utilisateur NLSP est créée comme indiqué au 6.4.1.1, avec type de données dem./ind. NLSP-CONNECT. Cette unité est placée dans le paramètre UN Userdata;

d) si l'attribut Protect_Connect_Params est VRAI, si l'attribut No_Header est FAUX et si l'attribut Param_Prot est FAUX, une SDT PDU contenant le paramètre NLSP Userdata, s'il est présent, est créée comme indiqué au 6.4.1.1 avec type de données dem./ind. NLSP-CONNECT. Cette unité est placée dans le paramètre UN Userdata;

e) si l'attribut Protect_Connect_Params est FAUX, le paramètre NLSP Userdata est placé dans le paramètre UN Userdata;

f) une CSC PDU est préparée avec:

1) marqueur UNC-UND libre;

2) identificateur SA-ID de l'association SA applicable placé dans le champ SA-ID;

3) marqueur SA-P libre;

4) contenu de CSC réglé selon le premier échange de CSC conformément aux procédures spécifiques des mécanismes telles que celles décrites au 10.3;

g) une demande UN-CONNECT doit être invoquée avec:

1) si l'attribut Param_Prot est présent, paramètre adresse UN appelée réglé à la valeur Peer_Adr, sinon adresse NLSP appelée;

2) si l'attribut Param_Prot est présent, paramètre adresse UN appelante réglé à la valeur adresse UN de l'entité NLSP locale, sinon adresse NLSP appelante;

3) paramètres sélection de confirmation de réception et sélection de données exprès UN réglés aux valeurs déterminées localement à partir des paramètres sélection de confirmation de réception et sélection de données exprès NLSP;

4) paramètre UN QOS réglé à une valeur déterminée localement à partir du paramètre NLSP QOS;

5) paramètre données d'utilisateur UN réglé comme indiqué aux points a) à d) ci-dessus;

6) paramètre UN authentification réglé à la valeur de la CSC PDU comme indiqué en e) ci-dessus;

h) la NLSPE appelante attend une confirmation UN-CONNECT comme indiqué au 8.5.2.4 ou une indication UN-DISCONNECT comme indiqué au 8.10.

A la fin de la mise en œuvre du protocole SA-P, le protocole NLSP attend un paramètre UN-DISCONNECT avec raison réglée à la valeur «disconnect-normal-condition». Après cette indication UN-DISCONNECT, la NLSPE appelée attend alors une indication UN-CONNECT comme indiqué au 8.5.2.2.

Les NLSPE appelante et NLSPE appelée doivent alors traiter les primitives NLSP et UN-CONNECT ultérieures comme indiqué aux 8.5.2.2 à 8.5.2.4.

8.5.4 Paramètres NLSP-CONNECT dans les paramètres UN-DATA

La séquence d'événements prévue est illustrée sur la Figure 8-3.

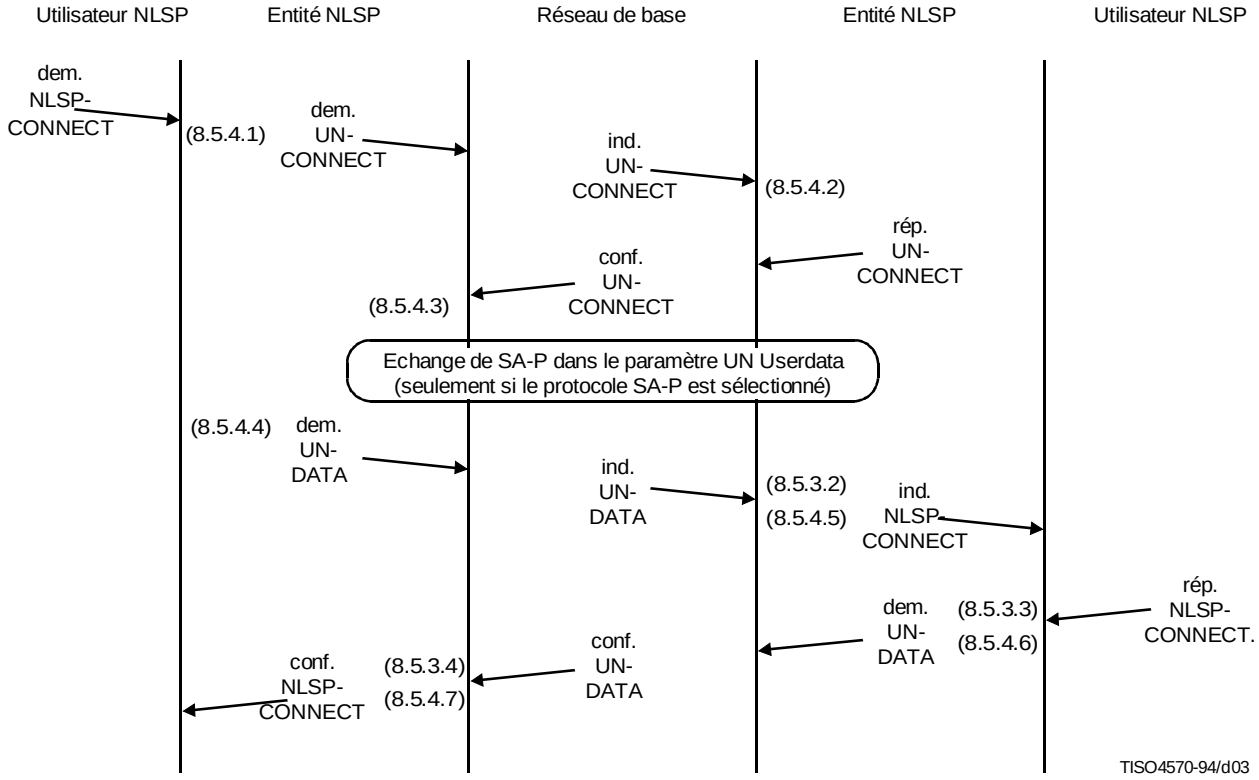


Figure 8-3 – Chronogramme de primitives de service pour les paramètres NLSP-CONNECT dans les paramètres UN-DATA

8.5.4.1 Demande NLSP-CONNECT

Lors d'une demande NLSP-CONNECT, si les paramètres NLSP-CONNECT doivent être acheminés dans les paramètres UN-DATA, la procédure suivante doit être mise en œuvre:

a) une CSC PDU doit être préparée avec:

1) marqueur UNC-UND positionné;

2) si le protocole SA-P dans la bande est sélectionné, marqueur SA-P positionné et champs SA-ID, longueur de contenu et contenu de CSC PDU non présents;

3) si le protocole SA-P dans la bande n'est pas sélectionné, marqueur SA-P libre, identificateur SA-ID réglé à la valeur Your_SA-ID et contenu de CSC PDU réglé selon le premier échange de CSC, conformément aux procédures spécifiques des mécanismes décrites au 10.3;

b) une demande UN-CONNECT doit être envoyée avec:

1) paramètre adresse UN appelée réglé à la valeur Peer_Adr;

2) paramètre adresse UN appelante réglé à la valeur adresse UN de l'entité NLSP locale;

3) paramètre sélection de confirmation de réception UN réglé à une valeur déterminée localement à partir du paramètre confirmation de réception NLSP;

4) paramètre sélection de données exprès UN réglé à une valeur déterminée localement à partir du paramètre sélection de données exprès NLSP;

5) paramètre UN QOS réglé à une valeur déterminée localement à partir du paramètre NLSP QOS;

6) paramètre données d'utilisateur UN vide;

7) paramètre UN authentification réglé à la valeur de la CSC PDU;

c) la NLSPE appelante doit attendre une confirmation UN-CONNECT comme indiqué au 8.5.4.3 ou une indication UN-DISCONNECT comme indiqué au 8.10.

8.5.4.2 Indication UN-CONNECT – UNC-UND positionné

A la réception d'une indication UN-CONNECT avec paramètre UN authentification contenant une CSC PDU avec marqueur UNC-UND positionné:

a) si le marqueur SA-P est libre, alors:

1) la NLSPE doit identifier, parmi les associations SA dont elle dispose, une association SA avec attribut My_SA-ID égal au champ SA-ID dans la CSC PDU reçue. Toutes les autres opérations se réfèrent à cette association SA identifiée;

2) le contenu de la CSC PDU doit être vérifié conformément aux procédures spécifiques des mécanismes telles que celles décrites au 10.3.

Si le marqueur SA-P est positionné ou libre, les procédures suivantes indiquées dans le présent paragraphe sont mises en œuvre.

b) La NLSPE doit préparer une CSC PDU avec:

1) marqueur UNC-UND positionné;

2) si le protocole SA-P dans la bande est sélectionné, champ SA-ID absent, sinon champ réglé à la valeur SA-ID reçue dans la CSC PDU;

3) si le protocole SA-P dans la bande est sélectionné, marqueur SA-P positionné, sinon libre;

4) si le protocole SA-P dans la bande est sélectionné, champs de contenu et de longueur de contenu de la CSC PDU non présents, sinon contenu de la CSC PDU réglé selon l'échange de CSC résultant des procédures spécifiques des mécanismes telles que celles définies au 10.3.

NOTE – Les procédures actuelles ne traitent pas le cas des mécanismes d'échange de CSC qui exigent plus d'un échange bilatéral de CSC PDU suivies, à titre facultatif, d'une SDT PDU.

c) La NLSPE doit alors répondre à l'aide d'une réponse UN-CONNECT avec:

1) paramètre adresse UN appelée réglé à la valeur adresse UN locale;

2) paramètres sélection de confirmation de réception et sélection de données exprès UN réglés à des valeurs déterminées localement à partir des paramètres contenus dans l'indication UN-CONNECT;

3) paramètre UN QOS réglé à une valeur déterminée localement à partir du paramètre UN QOS contenu dans l'indication UN-CONNECT;

4) paramètre données d'utilisateur UN vide;

5) paramètre UN authentification réglé à la valeur de la CSC PDU.

d) La NLSPE appelée doit attendre un échange de données de protocole SA-P ou une indication UN-DATA contenant une SDT PDU comme indiqué au 8.5.4.5 ou une indication UN-DISCONNECT comme indiqué au 8.10 ou un paramètre UN-RESET comme indiqué au 8.9.

8.5.4.3 Confirmation UN-CONNECT – UNC-UND positionné

A la réception d'une confirmation UN-CONNECT avec paramètre UN authentification contenant une CSC PDU de réponse avec marqueur UNC-UND positionné:

a) Il convient de vérifier que le marqueur SA-P dans la CSC PDU correspond à la sélection du protocole SA-P dans la bande.

b) Si le protocole SA-P n'est pas sélectionné:

1) le contenu de la CSC PDU est vérifié à l'aide des procédures spécifiques des mécanismes telles que celles décrites au 10.3;

2) la mise en œuvre des procédures continue comme indiqué au 8.5.4.4 c).

NOTE – Si le protocole SA-P n'est pas sélectionné et si le mécanisme d'échange de CSC exige l'échange de plus de deux CSC PDU, celles-ci sont échangées dans un paramètre UN-DATA avant la poursuite de la mise en œuvre des procédures d'établissement de connexion.

c) Le protocole SA-P dans la bande est sélectionné:

1) l'échange de données de protocole SA-P doit être effectué;

2) la NLSPE appelante attend la fin de la mise en œuvre du protocole SA-P comme indiqué au 8.5.4.4 ou une indication UN-DISCONNECT comme indiqué au 8.10 ou une indication UN-RESET comme indiqué au 8.9. Toute erreur dans le protocole SA-P doit être traitée comme une erreur conformément au 8.4.

8.5.4.4 Fin de mise en œuvre du protocole SA-P/absence de protocole SA-P

A la fin de la mise en œuvre du protocole SA-P:

a) Si le protocole SA-P est mis en œuvre avec succès, l'association SA établie est utilisée ultérieurement pour achever l'établissement de la connexion NLSP et de communications sûres comme indiqué dans les paragraphes qui suivent.

b) Si le protocole SA-P n'est pas mis en œuvre avec succès, la NLSPE appelante ou appelée doit invoquer une primitive UN-DISCONNECT et les procédures d'établissement de connexion NLSP doivent être abandonnées.

A la fin de la mise en œuvre du protocole SA-P ou à la suite d'une confirmation UN-CONNECT sans SA-P comme indiqué au 8.5.4.3 b):

c) Les paramètres NLSP-CONNECT suivants transmis au NLSP appelant lors de l'événement décrit au 8.5.4.1 doivent être placés dans une SDT PDU comme indiqué au 6.4.1.1, avec type de données «dem./ind. NLSP-CONNECT»:

- adresse NLSP appelante;
- adresse NLSP appelée;
- données d'utilisateur NLSP.

NOTE 1 – Les paramètres d'adresse NLSP sont acheminés sous une forme protégée même si l'attribut Param_Prot est FAUX.

d) La SDT PDU doit être transmise au fournisseur de service UN dans le paramètre UN Userdata d'une demande UN-DATA.

NOTE 2 – Cette opération peut constituer la troisième partie de l'échange de données d'authentification de l'entité homologue.

e) La NLSPE appelante attend une indication UN-DATA contenant une SDT PDU comme indiqué au 8.5.4.7 ou une indication UN-DISCONNECT comme indiqué au 8.10 ou une indication UN-RESET comme indiqué au 8.9.

A la fin de la mise en œuvre du protocole SA-P, la NLSPE appelée attend une indication UN-DATA contenant une SDT PDU comme indiqué au 8.5.4.5 ou une indication UN-DISCONNECT comme indiqué au 8.10 ou une indication UN-RESET comme indiqué au 8.9.

8.5.4.5 Réception d'une primitive UN-DATA contenant une SDT PDU au niveau de la NLSPE appelée

A la réception d'une indication UN-DATA contenant une PDU de transfert de données sûres au niveau de la NLSPE appelée, cette unité doit être vérifiée comme indiqué au 6.4.2.2.

NOTE – Cette opération peut constituer la troisième partie de l'échange de données d'authentification de l'entité homologue.

Il convient de vérifier que le champ de type de données dans la SDT PDU est dem./ind. NLSP-CONNECT.

Il convient de vérifier que l'adresse NLSP appelée est une adresse NLSP desservie par cette entité NLSP selon les décisions prises localement.

Il convient de vérifier que l'adresse NLSP appelante est une adresse NLSP contenue dans l'attribut SA-P Adr_Served.

Si une étiquette de sécurité est établie pour la connexion, cette étiquette est vérifiée en fonction de l'ensemble d'étiquettes autorisées dans l'attribut SA Label_Set.

L'indication NLSP-CONNECT doit être transmise à l'utilisateur NLSP appelé avec paramètres réglés comme suit:

a) paramètres adresse NLSP appelante, adresse NLSP appelée, données d'utilisateur NLSP réglés comme dans les champs de contenu de la SDT PDU reçue;

b) paramètres sélection de confirmation de réception et sélection de données exprès NLSP réglés à la valeur des paramètres UN équivalents dans la réponse UN-CONNECT envoyée conformément aux procédures indiquées au 8.5.4.2;

c) paramètre NLSP QOS «disponible» réglé à la valeur du paramètre UN QOS «sélectionné» par la NLSPE appelée dans la réponse UN-CONNECT envoyée conformément aux procédures indiquées au 8.5.4.2 et avec «valeur cible» et «valeur minimale acceptable» non spécifiées.

La NLSPE appelée doit attendre une réponse NLSP-CONNECT comme indiqué au 8.5.4.6 ou une demande NLSP-DISCONNECT comme indiqué au 8.10 ou une indication UN-DISCONNECT comme indiqué au 8.10 ou une indication UN-RESET comme indiqué au 8.9.

8.5.4.6 Réponse NLSP-CONNECT

A la réception d'une réponse NLSP-CONNECT, les paramètres adresse NLSP appelée et données d'utilisateur NLSP doivent être placés dans une SDT PDU comme indiqué au 6.4.1.1, avec type de données «rép./conf. NLSP-CONNECT».

Cette SDT PDU doit être transmise au fournisseur de service UN dans le paramètre UN Userdata d'une demande UN-DATA.

La NLSPE appelée a maintenant terminé ses procédures d'établissement de connexion NLSP.

8.5.4.7 Réception d'une primitive UN-DATA contenant une SDT PDU au niveau de la NLSPE appelante

A la réception d'une indication UN-DATA contenant une SDT PDU, cette unité doit être vérifiée comme indiqué au 6.4.2.1. Il convient de vérifier que le champ de type de données est rép./conf. NLSP-CONNECT.

Il convient de vérifier que l'adresse NLSP appelée est une adresse NLSP contenue dans l'attribut SA Adr_Served.

Une confirmation NLSP-CONNECT est envoyée à l'utilisateur NLSP avec paramètres réglés comme suit:

a) paramètres adresse NLSP appelée, données d'utilisateur NLSP, s'ils sont présents, réglés comme dans les champs de contenu de la SDT PDU reçue;

b) paramètres sélection de confirmation de réception et sélection de données exprès NLSP réglés à la valeur des paramètres UN équivalents dans la confirmation UN-CONNECT envoyée conformément aux procédures indiquées au 8.5.4.3;

c) paramètre NLSP QOS réglé à la valeur du paramètre UN QOS reçu dans la confirmation UN-CONNECT conformément aux procédures décrites au 8.5.3.

La NLSPE appelante a maintenant terminé ses procédures d'établissement de connexion NLSP.

8.6 Fonctions NLSP-DATA

8.6.1 Demande NLSP-DATA

A la réception d'une demande NLSP-DATA, si l'attribut No_Header est VRAI, le paramètre données d'utilisateur NLSP doit être encapsulé comme indiqué au 6.4.1.2. Ce paramètre est placé dans le paramètre données d'utilisateur UN d'une

demande UN-DATA et le paramètre demande de confirmation NLSP est copié dans le paramètre UN-DATA équivalent. Ce paramètre doit alors être transmis au fournisseur de service UN.

A la réception d'une demande NLSP-DATA, si l'attribut No_Header est FAUX:

a) conformément aux décisions prises localement, la NLSPE doit segmenter les données d'utilisateur NLSP (si l'association SA l'exige);

b) pour chaque segment, une SDT PDU doit être créée comme indiqué au 6.4.1.1, avec type de données «dem./ind. NLSP-DATA» contenant:

   1) le segment de données d'utilisateur NLSP;

   2) le marqueur Last/Not last (champ complet/champ partiel) réglé à 0 pour le dernier segment et à 1 pour tous les segments précédents;

   3) le champ de contenu demande de confirmation NLSP

      i) si la demande de confirmation NLSP indiquant «confirmation de réception demandée» est présente dans la demande NLSP-DATA;

      ii) si ce segment est le dernier; et

      iii) si l'attribut Param_Prot est VRAI;

c) la SDT PDU pour chaque segment doit être placée dans le paramètre UN Userdata d'une demande UN-DATA;

d) le paramètre demande de confirmation UN de la demande UN-DATA indiquant «confirmation de réception demandée» doit être présent:

   1) si la demande de confirmation NLSP est indiquée dans la demande NLSP-DATA;

   2) si ce segment est le dernier; et

   3) si l'attribut Param_Prot est FAUX

      sinon, le paramètre demande de confirmation UN doit indiquer «confirmation de réception non demandée»;

e) la primitive de demande UN-DATA pour chaque segment doit être transmise au fournisseur de service UN.

8.6.2 Données protégées dans une indication UN-DATA suivant l'établissement de la connexion

A la réception d'une indication UN-DATA, si l'attribut No_Header est VRAI, le paramètre données d'utilisateur UN doit être décapsulé comme indiqué au 6.4.2.2. Ce paramètre est placé dans le paramètre données d'utilisateur NLSP d'une indication NLSP-DATA et le paramètre demande de confirmation UN est copié dans le paramètre d'indication NLSP-DATA équivalent. L'indication NLSP-DATA doit alors être transmise à l'utilisateur de service NLSP.

A la réception d'une indication UN-DATA, si l'attribut No_Header est FAUX:

a) la SDT PDU dans le paramètre données d'utilisateur UN doit être vérifiée comme indiqué au 6.4.2.1;

b) si le champ de type de données n'est «lié à aucune primitive de service NLSP», la SDT PDU doit être traitée comme indiqué au 8.11 et non comme indiqué ci-dessous;

c) si le champ de type de données est «dem./ind. NLSP-DATA-ACKNOWLEDGE», la SDT PDU doit être traitée comme indiqué au 8.9.2 et non comme indiqué ci-dessous;

d) si le champ de type de données est «dem./ind. NLSP-DISCONNECT», la SDT PDU doit être traitée comme indiqué au 8.10.2 et non comme indiqué ci-dessous;

e) dans le cas contraire, il convient de vérifier que le champ de type de données est NLSP-DATA et le traiter comme suit;

f) si le marqueur Last/Not last (champ complet/champ partiel) dans la SDT PDU est réglé à 1 (champ partiel), le champ de contenu données d'utilisateur NLSP dans la SDT PDU est ajouté à tout paramètre données d'utilisateur NLSP précédent qui fait partie de la même demande/indication NLSP-DATA et est conservé par la NLSPE pour utilisation ultérieure;

g) si le marqueur Last/Not last dans la SDT PDU est réglé à 0 (champ complet):

1) le champ de contenu données d'utilisateur NLSP dans la SDT PDU est ajouté à tout paramètre données d'utilisateur NLSP précédent qui fait partie de la même demande/indication NLSP-DATA et est placé dans le paramètre données d'utilisateur NLSP d'une indication NLSP-DATA;

2) si l'attribut Param_Prot est VRAI, la demande de confirmation NLSP dans l'indication NLSP-DATA doit indiquer «confirmation de réception demandée» si le champ de contenu de demande de confirmation est présent dans la SDT PDU;

3) si l'attribut Param_Prot est FAUX, la demande de confirmation UN dans l'indication UN-DATA reçue est copiée dans le paramètre équivalent de l'indication NLSP-DATA;

4) l'indication NLSP-DATA est transmise à l'utilisateur NLSP.

8.7 Fonctions NLSP-EXPEDITED-DATA (données exprès NLSP)

8.7.1 Demande NLSP-EXPEDITED-DATA

A la réception d'une demande NLSP-EXPEDITED-DATA, si l'attribut No_Header est VRAI, le paramètre données d'utilisateur NLSP doit être encapsulé comme indiqué au 6.4.1.2. Ce paramètre est placé dans le paramètre données d'utilisateur UN d'une demande UN-EXPEDITED-DATA. La demande UN-EXPEDITED-DATA est alors transmise au fournisseur de service UN.

A la réception d'une demande NLSP-EXPEDITED-DATA, si l'attribut No_Header est FAUX:

a) conformément aux décisions prises localement, la NLSPE doit segmenter les données d'utilisateur NLSP (si l'association SA l'exige);

b) pour chaque segment, une SDT PDU doit être créée comme indiqué au 6.4.1.1, avec type de données «dem./ind. NLSP-EXPEDITED-DATA» contenant:

1) le segment de données d'utilisateur NLSP;

2) le marqueur Last/Not last (champ complet/champ partiel) réglé à 0 pour le dernier segment et à 1 pour tous les segments précédents;

3) la SDT PDU pour chaque segment doit être placée dans le paramètre données d'utilisateur UN d'une primitive UN-EXPEDITED-DATA;

c) la primitive de demande UN-EXPEDITED-DATA pour chaque segment doit être transmise au fournisseur de service UN.

NOTE – Lors de l'utilisation de la SDT PDU, étant donné que la fonction d'encapsulation peut accroître la longueur des données, la longueur restreinte du champ de données d'utilisateur peut exiger que les données exprès protégées soient à nouveau segmentées lors de leur passage par le réseau de base.

8.7.2 Indication UN-EXPEDITED-DATA

A la réception d'une indication UN-EXPEDITED-DATA, si l'attribut No_Header est VRAI, le paramètre données d'utilisateur NLSP doit être décapsulé comme indiqué au 6.4.2.2. Ce paramètre est placé dans le paramètre données d'utilisateur NLSP d'une indication NLSP-EXPEDITED-DATA. L'indication NLSP-EXPEDITED-DATA est alors transmise au fournisseur de service NLSP.

A la réception d'une indication UN-EXPEDITED-DATA, si l'attribut No_Header est FAUX:

NOTE – Lors de l'utilisation de la SDT PDU, étant donné que la fonction d'encapsulation peut accroître la longueur des données, la longueur restreinte du champ de données d'utilisateur peut exiger que la SDT PDU soit réassemblée à partir de plusieurs demandes NLSP-EXPEDITED-DATA avant d'être entièrement traitée.

a) La SDT PDU dans le paramètre données d'utilisateur UN doit être vérifiée comme indiqué au 6.4.2.1. Il convient de vérifier que le type de données dans la SDT PDU est dem./ind. NLSP-EXPEDITED-DATA.

b) Si le marqueur «Last/Not last» (champ complet/champ partiel) dans la SDT PDU est réglé à 1 (champ partiel), le champ de contenu données d'utilisateur NLSP dans la SDT PDU est ajouté à tout paramètre données d'utilisateur NLSP précédent qui fait partie de la même demande/indication NLSP-EXPEDITED-DATA et est conservé par la NLSPE pour utilisation ultérieure.

c) Si le marqueur «Last/Not last» (champ complet/champ partiel) dans la SDT PDU est réglé à 0 (champ complet):

1) le champ de contenu données d'utilisateur NLSP dans la SDT PDU est ajouté à tout paramètre données d'utilisateur NLSP précédent qui fait partie de la même demande/indication NLSP-EXPEDITED-DATA et est placé dans le paramètre données d'utilisateur NLSP d'une indication NLSP-EXPEDITED-DATA;

2) la primitive de service indication NLSP-EXPEDITED-DATA est transmise à l'utilisateur NLSP.

8.8 Fonctions RESET (réinitialisation)

L'un quelconque des événements liés aux fonctions NLSP ou UN-RESET et énumérés ci-dessous a priorité sur tout échange de CSC PDU, tout échange de données de protocole SA-P ou tout échange de tests en cours.

8.8.1 Demande NLSP-RESET

A la réception d'une demande NLSP-RESET, une demande UN-RESET doit être émise avec les mêmes valeurs de paramètre.

Tout paramètre données d'utilisateur NLSP segmenté conservé conformément aux procédures décrites aux 8.6 ou 8.7 doit être rejeté.

La NLSPE doit attendre une confirmation UN-RESET comme indiqué au 8.8.2 ou une demande NLSP-DISCONNECT ou une indication UN-DISCONNECT comme indiqué au 8.10. La NLSPE rejette toutes les primitives UN-DATA et UN-DATA-ACKNOWLEDGE jusqu'à la réception d'une primitive confirmation UN-RESET ou DISCONNECT.

8.8.2 Confirmation UN-RESET suivant une demande NLSP-RESET

A la réception d'une confirmation UN-RESET suivant une demande NLSP-RESET comme indiqué au 8.8.1, une confirmation NLSP-RESET doit être émise avec les mêmes valeurs de paramètre.

NOTE – Il peut être nécessaire de réinitialiser certains mécanismes de sécurité car des données peuvent avoir été perdues. Des mécanismes de séquencement d'intégrité doivent, en particulier, pouvoir empêcher des attaques consistant à répéter des messages dans un but malveillant, même après la perte de données. On peut, à cet effet, utiliser l'échange de CSC PDU décrit ci -dessous.

Si l'attribut SA «Initiator» (entité initiatrice) est VRAI, la NLSPE doit déclencher un échange de commandes CSC comme indiqué au 8.12.1; sinon, la NLSPE doit attendre une primitive UN-DATA contenant une CSC PDU comme indiqué au 8.12.2.

8.8.3 Indication UN-RESET

A la réception d'une indication UN-RESET pendant les procédures d'établissement de connexion NLSP décrites au 8.5, une demande UN-DISCONNECT et une indication NLSP-DISCONNECT doivent être émises conformément au service de réseau OSI et les procédures d'établissement de connexion doivent être abandonnées.

A la réception d'une indication UN-RESET suivant la fin de l'établissement de connexion NLSP:

a) une indication NLSP-RESET doit être émise avec les mêmes valeurs de paramètre;

b) tout paramètre données d'utilisateur NLSP segmenté conservé conformément aux procédures décrites aux 8.6 et 8.7 doit être rejeté;

c) la NLSPE doit attendre une réponse NLSP-RESET comme indiqué au 8.8.4 ou une demande NLSP-DISCONNECT ou une indication UN-DISCONNECT comme indiqué au 8.10. La NLSPE rejette toutes les primitives UN-DATA et UN-DATA-ACKNOWLEDGE jusqu'à la réception d'une réponse NLSP-RESET ou DISCONNECT.

8.8.4 Réponse NLSP-RESET suivant une indication UN-RESET

A la réception d'une réponse NLSP-RESET suivant une indication UN-RESET, comme indiqué au 8.8.3, une réponse UN-RESET doit être émise.

NOTE – Il peut être nécessaire de réinitialiser certains mécanismes de sécurité car des données peuvent avoir été perdues. Des mécanismes de séquencement d'intégrité doivent, en particulier, pouvoir empêcher des attaques consistant à répéter des messages dans un but malveillant, même après la perte de données. On peut, à cet effet, utiliser l'échange de CSC PDU décrit ci -dessous.

Si l'attribut SA «Initiator» (entité initiatrice) est VRAI, la NLSPE doit déclencher un échange de commandes CSC comme indiqué au 8.12.1; sinon, le protocole NLSP doit attendre un paramètre UN-DATA contenant une CSC PDU comme indiqué au 8.12.2.

8.8.5 Réinitialisation déclenchée par le protocole NLSP

Lors d'une réinitialisation déclenchée à la suite d'un événement lié au protocole NLSP (par exemple, un échec de vérification comme indiqué au 8.4):

a) tout paramètre données d'utilisateur NLSP segmenté conservé conformément aux procédures décrites au 8.6 ou 8.7 doit être rejeté;

b) une indication NLSP-RESET doit être transmise à l'utilisateur de service NLSP avec paramètres entité appelante NLSP et raison NLSP réglés à une valeur déterminée localement;

c) une demande UN-RESET doit être transmise au fournisseur de service UN avec paramètre raison UN réglé à une valeur déterminée localement;

d) la NLSPE doit attendre une réponse NLSP-RESET comme indiqué au 8.8.6 et une confirmation UN-RESET comme indiqué au 8.8.7. Une demande NLSP-DISCONNECT ou une indication UN-DISCONNECT, comme indiqué au 8.10, peut être également reçue;

e) la NLSPE doit rejeter toutes les primitives UN-DATA et UN-DATA-ACKNOWLEDGE jusqu'à la réception d'une primitive de confirmation UN-RESET ou de toute primitive DISCONNECT;

f) la NLSPE doit rejeter toutes les primitives NLSP-DATA et NLSP-DATA-ACKNOWLEDGE jusqu'à la réception d'une primitive de réponse NLSP-RESET ou de toute primitive DISCONNECT.

8.8.6 Réponse NLSP-RESET suivant une réinitialisation déclenchée par le protocole NLSP

Aucune autre action n'est nécessaire en cas de réponse NLSP-RESET suivant une réinitialisation déclenchée par le protocole NLSP.

8.8.7 Primitive de confirmation UN-RESET suivant une réinitialisation déclenchée par le protocole NLSP

NOTE – Il peut être nécessaire de réinitialiser certains mécanismes de sécurité car des données peuvent avoir été perdues. Des mécanismes de séquencement d'intégrité doivent, en particulier, pouvoir empêcher des attaques consistant à répéter des messages dans un but malveillant, même après la perte de données. On peut, à cet effet, utiliser l'échange de CSC PDU décrit ci -dessous.

En cas de primitive de confirmation UN-RESET suivant une réinitialisation déclenchée par le protocole NLSP, si l'attribut SA Initiator (entité initiatrice) est VRAI, la NLSPE doit déclencher un échange de commandes CSC comme indiqué au 8.12.1; sinon, la NLSPE doit attendre une primitive UN-DATA contenant une CSC PDU comme indiqué au 8.12.2.

8.9 Fonctions NLSP-DATA-ACKNOWLEDGE

8.9.1 Demande NLSP-DATA-ACKNOWLEDGE

A la réception d'une demande NLSP-DATA-ACKNOWLEDGE, si l'attribut No_Header est VRAI ou si l'attribut Param_Prot est FAUX, une demande UN-DATA-ACKNOWLEDGE est transmise au fournisseur de service UN.

A la réception d'une demande NLSP-DATA-ACKNOWLEDGE, si l'attribut No_Header est FAUX et si l'attribut Param_Prot est VRAI:

a) une SDT PDU doit être créée comme indiqué au 6.4.1.1, avec type de données «dem./ind. NLSP-DATA-ACKNOWLEDGE» ne contenant aucun champ de contenu additionnel;

b) la SDT PDU doit être transmise au fournisseur de service UN sous la forme de données d'utilisateur UN dans une primitive de demande UN-DATA.

8.9.2 Primitive NLSP-DATA-ACKNOWLEDGE protégée dans une indication UN-DATA

Si une SDT PDU est reçue dans une indication UN-DATA, avec type de données réglé à la valeur NLSP-DATA-ACKNOWLEDGE comme indiqué au 8.6.2 c):

a) il convient de vérifier que la SDT PDU ne contient aucun champ de contenu lié aux paramètres de service NLSP;

b) une indication NLSP-DATA-ACKNOWLEDGE doit être transmise à l'utilisateur NLSP.

8.9.3 Indication UN-DATA-ACKNOWLEDGEMENT

A la réception d'une indication UN-DATA-ACKNOWLEDGEMENT:

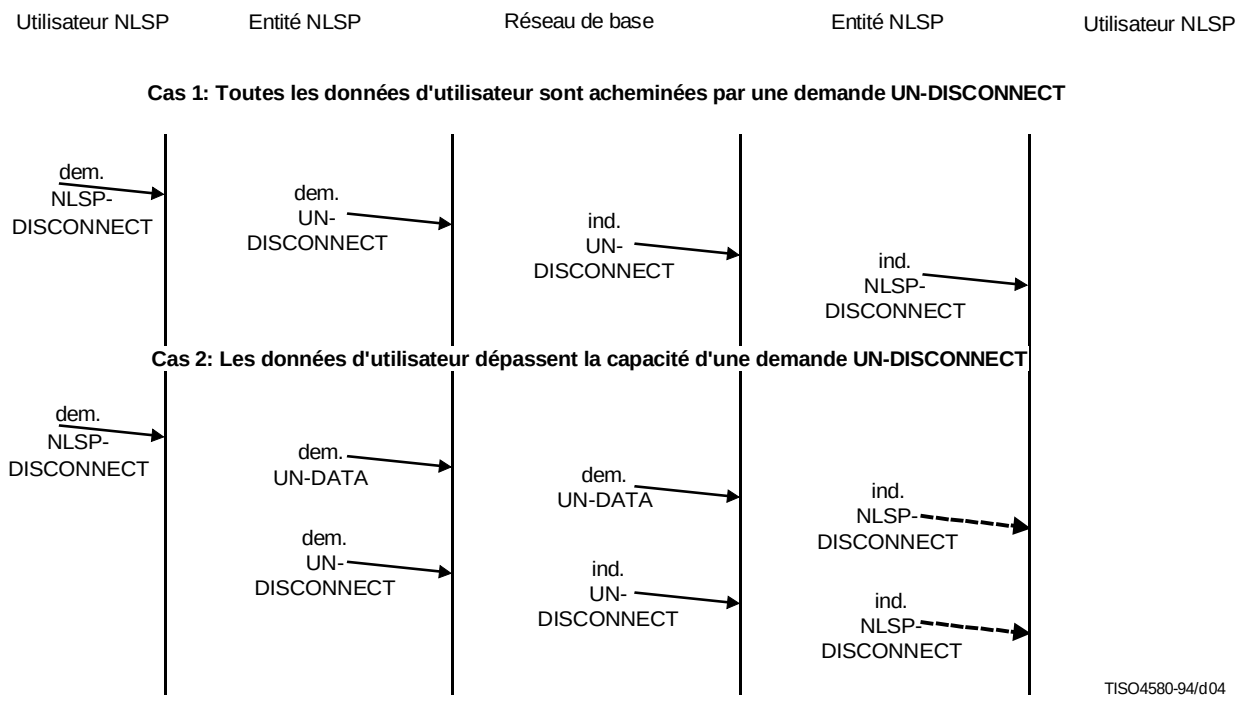
a) la NLSPE doit vérifier que l'attribut No_Header est VRAI ou que l'attribut Param_Prot est FAUX;

b) une indication NLSP-DATA-ACKNOWLEDGEMENT doit être transmise à l'utilisateur NLSP.

8.10 Primitive NLSP-DISCONNECT

L'un quelconque des événements liés à une primitive NLSP-DISCONNECT ou UN-DISCONNECT et énumérés ci-dessous a priorité sur tout échange de CSC PDU, de données de protocole SA-P ou de tests en cours.

Les procédures applicables à une déconnexion déclenchée par l'utilisateur NLSP sont illustrées sur la Figure 8-4.



NOTE – Une primitive NLSP-DISCONNECT peut être émise à l'un ou l'autre des points indiqués.

Figure 8-4 – Chronogramme de primitives de service pour la fonction NLSP-DISCONNECT

8.10.1 Demande NLSP-DISCONNECT

A la réception d'une demande NLSP-DISCONNECT pendant les procédures d'établissement de connexion NLSP comme indiqué au 8.5, une demande UN-DISCONNECT doit être émise conformément au service de réseau OSI (c'est-à-dire si l'établissement d'une connexion UN a commencé) et les procédures d'établissement de connexion doivent être abandonnées. Si l'attribut Protect_Connect_Params est VRAI, les paramètres de toute demande UN-DISCONNECT doivent être déterminés localement, sinon les paramètres de demande NLSP-DISCONNECT doivent être copiés dans les paramètres de demande UN-DISCONNECT équivalents.

NOTE – Si une demande NLSP-DISCONNECT est émise pendant l'établissement de la connexion et si l'attribut Protect_Connect_Params est sélectionné, les paramètres de demande NLSP-DISCONNECT seront rejetés.

A la réception d'une demande NLSP-DISCONNECT suivant l'établissement de la connexion NLSP:

a) si l'attribut Protect_Connect_Params est VRAI et si l'attribut No_Header est VRAI, tout paramètre données d'utilisateur NLSP doit être encapsulé comme indiqué au 6.4.1.2. Ce paramètre est placé dans le paramètre données d'utilisateur UN d'une demande UN-DISCONNECT. Les autres paramètres de demande NLSP-DISCONNECT sont copiés dans les paramètres de demande UN-DISCONNECT équivalents;

b) si l'attribut Protect_Connect_Params est VRAI, si l'attribut No_Header est FAUX et si l'attribut Param_Prot est VRAI, une SDT PDU contenant tous les paramètres de demande NLSP-DISCONNECT comme indiqué au 6.4.1.1 est émise, avec type de données «dem./ind. NLSP-DISCONNECT». Cette unité est placée dans un paramètre données d'utilisateur UN. Les autres paramètres UN-DISCONNECT sont déterminés localement;

c) si le paramètre données d'utilisateur NLSP est présent, si l'attribut Protect_Connect_Params est VRAI, si l'attribut No_Header est FAUX et si l'attribut Params_Prot est FAUX, une SDT PDU contenant le paramètre données d'utilisateur NLSP comme indiqué au 6.4.1.1 est créée, avec type de données «dem./ind. NLSP-DISCONNECT». Cette unité est placée dans un paramètre données d'utilisateur UN. Les autres paramètres de demande NLSP-DISCONNECT sont copiés dans les paramètres de demande UN-DISCONNECT équivalents;

d) si l'attribut Protect_Connect_Params est FAUX, tous les paramètres NLSP-DISCONNECT sont copiés dans les paramètres de demande UN-DISCONNECT équivalents;

NOTE – On admet implicitement que les limites qui s'appliquent à la longueur du paramètre données d'utilisateur UN s'appliquent également au paramètre données d'utilisateur NLSP.

e) si, à la suite de b) ou c) ci-dessus, le paramètre données d'utilisateur UN résultant est supérieur à la longueur maximale du paramètre données d'utilisateur UN de la demande UN-DISCONNECT, ce paramètre doit être envoyé plutôt dans le paramètre données d'utilisateur UN d'une demande UN-DATA et transmis au fournisseur de service UN. Le paramètre données d'utilisateur UN pour la demande UN-DISCONNECT doit être vide;

NOTE – L'équipement mis en œuvre doit attendre que cette primitive UN-DATA traverse le réseau de base avant de procéder à l'envoi de la demande UN-DISCONNECT comme indiqué au paragraphe suivant. La durée de cette attente est déterminée localement.

f) une demande UN-DISCONNECT doit être envoyée avec paramètres réglés comme indiqué ci-dessus.

8.10.2 Paramètres NLSP-DISCONNECT protégés dans une indication UN-DATA

Si une SDT PDU est reçue dans une indication UN-DATA, avec type de données réglé à la valeur NLSP-DISCONNECT, comme indiqué au 8.6.2 d):

a) la NLSPE vérifie que l'attribut Protect_Connect_Params est VRAI et que l'attribut No_Header est FAUX;

b) tous les champs de contenu contenant des paramètres de service NLSP sont copiés dans les paramètres NLSP-DISCONNECT équivalents et l'entité NLSP appelante est réglée à la valeur utilisateur NS;

c) la NLSPE conserve les paramètres NLSP-DISCONNECT réglés comme ci-dessus, attend une indication UN-DISCONNECT ou émet immédiatement une indication NLSP-DISCONNECT. Le choix relève du domaine local.

8.10.3 Indication UN-DISCONNECT

A la réception d'une indication UN-DISCONNECT pendant les procédures d'établissement de connexion NLSP comme indiqué au 8.5, une indication NLSP-DISCONNECT doit être émise conformément au service de réseau OSI et les procédures d'établissement de connexion doivent être abandonnées. Les paramètres d'indication UN-DISCONNECT doivent être copiés dans les paramètres équivalents de toute indication NLSP-DISCONNECT ou, si l'attribut Protect_Connect_Params est VRAI, ils doivent être réglés conformément aux décisions prises localement.

Dans les autres cas, à la réception d'une indication UN-DISCONNECT suivant l'établissement d'une connexion NLSP, avec paramètre données d'utilisateur UN non vide:

a) si l'attribut Protect_Connect_Params est VRAI et si l'attribut No_Header est VRAI, le paramètre données d'utilisateur UN doit être décapsulé comme indiqué au 6.4.2.2. Ce paramètre est placé dans le paramètre données d'utilisateur NLSP d'une indication NLSP-DISCONNECT. Les autres paramètres d'indication NLSP-DISCONNECT doivent être réglés à la valeur des paramètres de l'indication UN-DISCONNECT équivalents;

b) si l'attribut Protect_Connect_Params est VRAI, si l'attribut No_Header est FAUX et si l'attribut Param_Prot est VRAI, la SDT PDU dans le paramètre données d'utilisateur UN doit être vérifiée comme indiqué au 6.4.2.1. Il convient de vérifier que le type de données est dem./ind. NLSP-DISCONNECT. Tous les champs de contenu relatifs aux paramètres NLSP-DISCONNECT sont copiés dans ces paramètres;

c) si l'attribut Protect_Connect_Params est VRAI, si l'attribut No_Header est FAUX et si l'attribut Params_Prot est FAUX, la SDT PDU dans le paramètre données d'utilisateur UN est vérifiée comme indiqué au 6.4.2.1. Il convient de vérifier que le type de données est NLSP-DISCONNECT. La présence du champ de contenu données d'utilisateur doit être vérifiée puis ce champ doit être copié dans le paramètre données d'utilisateur NLSP d'une indication NLSP-DISCONNECT. Les autres paramètres d'indication UN-DISCONNECT sont copiés dans les paramètres d'indication NLSP-DISCONNECT équivalents;

d) si l'attribut Protect_Connect_Params est FAUX, tous les paramètres UN-DISCONNECT sont copiés dans les paramètres d'indication NLSP-DISCONNECT équivalents;

e) l'indication NLSP-DISCONNECT doit être transmise à l'utilisateur NLSP.

Dans les autres cas, lors d'une indication UN-DISCONNECT suivant l'établissement d'une connexion NLSP avec paramètre donnnées d'utilisateur NLSP vide:

a) si la NLSPE attend une indication UN-DISCONNECT suivant un paramètre NLSP-DISCONNECT protégé dans une indication UN-DATA [voir 8.10.2 c)], les champs de paramètre NLSP protégés doivent être placés dans l'indication NLSP-DISCONNECT. Les autres paramètres d'indication NLSP-DISCONNECT doivent être réglés à la valeur des paramètres d'indication UN-DISCONNECT équivalents;

b) sinon, les paramètres d'indication UN-DISCONNECT doivent être copiés dans les paramètres d'indication NLSP-DISCONNECT équivalents;

c) l'indication NLSP-DISCONNECT doit être transmise à l'utilisateur NLSP à moins qu'une telle indication n'ait déjà été émise.

Les attributs SA peuvent être supprimés localement à la suite de toute primitive UN-DISCONNECT si l'attribut Retain_On_Disconnect est FAUX.

8.10.4 Déconnexion déclenchée par le protocole NLSP

En cas d'échec de mise en œuvre d'un protocole SA-P ou de toute autre vérification, les indications NLSP-DISCONNECT et les demandes UN-DISCONNECT sont transmises à l'utilisateur NLSP et au réseau de base comme indiqué au 8.4.

La Figure 8-5 donne un exemple qui illustre une déconnexion déclenchée par le protocole NLSP en raison de l'échec de mise en œuvre d'un protocole SA-P.

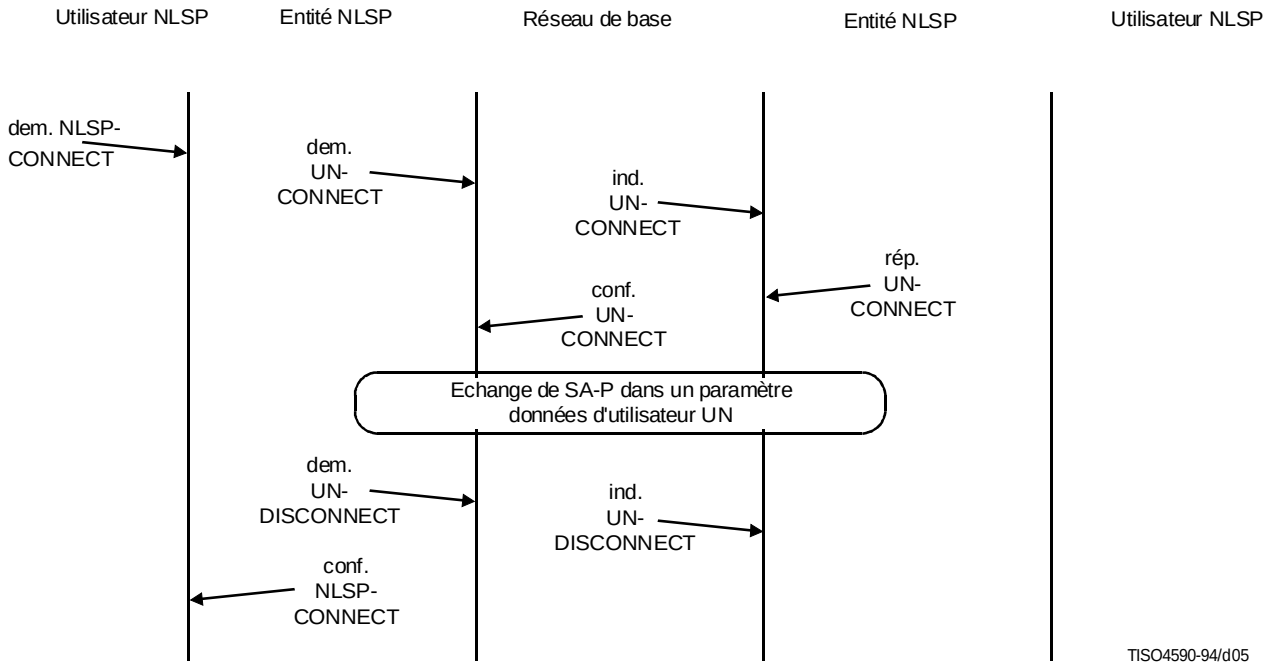


Figure 8-5 – Déconnexion déclenchée par le protocole NLSP à la suite de l'échec de mise en œuvre d'un protocole SA-P

8.11 Autres fonctions

Les procédures suivantes sont déclenchées en cas d'événements programmés ou d'autres événements externes.

8.11.1 Modification d'attributs SA dynamiques

La NLSPE peut modifier des attributs SA dynamiques (voir l'Annexe G) à tout moment pendant la durée d'une connexion. Aucune modification d'attributs SA dynamiques ne doit avoir d'incidence sur les services de sécurité assurés. Un échange de CSC PDU ou de données de protocole SA-P (à l'aide de SA PDU ou SDT PDU avec type de données protocole SA) est effectué dans le paramètre données d'utilisateur d'une primitive UN-DATA ou des moyens externes sont utilisés à cet effet. Cet échange est transparent pour l'utilisateur NLSP et aucune primitive NLSP n'est définie pour l'invoquer.

NOTE – Par exemple, cette procédure pourrait être mise en œuvre à intervalles réguliers au cours d'une connexion (par exemple, toutes les heures ou toutes les 10 000 PDU de données sûres) pour l'échange de clés.

Lorsque le transfert de données est effectué avec attribut No_Header sélectionné, une primitive UN-RESET doit être envoyée avant l'échange de CSC PDU comme indiqué au 8.8.5.

Les procédures d'échange de CSC PDU doivent être celles décrites au 8.12. Un exemple de protocole SA-P qui inclut les procédures à appliquer pour modifier les attributs SA est donné dans l'Annexe C.

8.11.2 Echange de tests de sécurité

Ces procédures doivent être utilisées pour tester le fonctionnement des aspects cryptographiques d'une association SA.

Elles ne peuvent être invoquées que dans les états où des primitives NLSP-DATA peuvent être envoyées dans des primitives UN-DATA (c'est-à-dire après la fin d'établissement de la connexion NLSP, avant toute procédure de déconnexion et non au cours des procédures de réinitialisation).

Toute primitive DISCONNECT, RESET et tout échange de CSC PDU ou de données de protocole SA-P aura priorité sur un échange de tests.

NOTE – L'utilisation de cette facilité sera déterminée localement. Les modes d'application possibles sont les suivants:

a) non-utilisation;

b) utilisation à la suite d'un échange de clés;

c) utilisation périodique, à un moment déterminé localement.

8.11.2.1 Invocation de l'échange de tests

Lors de l'invocation d'un échange de tests:

a) un champ de données de test doit être créé avec marqueur de direction libre (réglé à 0) et données de test réglées à la valeur données aléatoires;

b) une SDT PDU doit être créée comme indiqué au 6.4.1.1, avec type de données «n'étant lié à aucune primitive de service NLSP» et contenant le champ de données de test;

c) cette PDU doit être envoyée dans le paramètre données d'utilisateur UN d'une primitive UN-DATA, avec confirmation de réception UN indiquant «confirmation de réception non demandée».

8.11.2.2 Primitive UN-DATA avec SDT PDU contenant des données de test

A la réception d'une primitive UN-DATA contenant une SDT PDU avec type de données réglé à 0 (n'étant lié à aucune primitive de service NLSP) comme indiqué au 8.6.2 b), si la SDT PDU contient des données de test, elle doit être traitée comme suit:

a) si le marqueur de direction dans le champ de données de test est libre, une nouvelle SDT PDU doit être créée comme indiqué au 6.4.1.1, avec type de données «n'étant lié à aucune primitive de service NLSP» et contenant un champ de données de test avec marqueur de direction positionné et données réglées à la valeur données aléatoires reçues. Cette PDU doit être renvoyée dans le paramètre données d'utilisateur UN d'une primitive UN-DATA, avec confirmation de réception UN indiquant «confirmation de réception non demandée»;

b) si le marqueur de direction dans les données de test est positionné, il convient de vérifier que les données de test reçues sont identiques aux données de test précédemment envoyées. Sinon, la NLSPE doit mettre en œuvre les fonctions d'erreur définies au 8.4.

8.11.3 Remplissage de trafic

Des primitives UN-DATA additionnelles contenant des PDU de transfert de données sûres avec un simple remplissage de trafic peuvent être envoyées pour dissimuler la présence de données d'utilisateur.

Toutes les entités NLSP doivent pouvoir recevoir des PDU de transfert de données sûres avec un tel remplissage de trafic.

L'utilisation de cette facilité est laissée à l'appréciation de l'entité NLSP locale et est transparente pour l'utilisateur de service NLSP.

8.11.3.1 Invocation du remplissage de trafic

Lors de l'invocation du remplissage de trafic:

a) une SDT PDU avec type de données «n'étant lié à aucune primitive de service NLSP» et ne contenant aucun champ de contenu additionnel autre que ceux nécessaires au titre du 6.4.1.1 doit être créée comme indiqué au 6.4.1.1;

b) cette PDU doit être envoyée dans le paramètre données d'utilisateur UN d'une primitive UN-DATA avec confirmation de réception UN indiquant «confirmation de réception non demandée».

8.11.3.2 Primitive UN-DATA avec SDT PDU ne contenant aucun champ de contenu additionnel

A la réception d'une primitive UN-DATA contenant une SDT PDU avec type de données réglé à 0 (n'étant lié à aucune primitive de service NLSP) comme indiqué au 8.6.2 b), si la SDT PDU ne contient aucun champ de contenu autre que ceux généralement nécessaires au titre de l'article 6, cette SDT PDU doit être ignorée.

8.12 Authentification de l'entité homologue

Les procédures définies aux 8.12.1 et 8.12.2 peuvent être invoquées:

- à la suite d'une primitive UN-RESET ou NLSP-RESET comme indiqué au 8.8;
- à des intervalles de temps décidés localement,

pour assurer l'authentification de l'entité homologue ou modifier des attributs SA dynamiques.

L'échange de CSC PDU pendant l'établissement d'une connexion est décrit au 8.5.

Les demandes NLSP-DATA ou NLSP-EXPEDITED-DATA ne doivent pas être satisfaites avant la fin d'un échange de commandes CSC.

Toute primitive RESET ou DISCONNECT aura priorité sur l'échange de commandes CSC.

8.12.1 Invocation d'échange de commandes CSC

Lors de l'invocation d'un échange de commandes CSC, une CSC PDU doit être créée avec:

a) marqueurs UNC-UND et SA-P libres;

b) identificateur SA-ID réglé à la valeur Your_SA-ID;

c) contenu réglé selon le premier échange de commandes CSC conformément aux procédures spécifiques des mécanismes telles que celles décrites au 10.3.

Cette CSC PDU doit être envoyée dans le paramètre données d'utilisateur UN d'une primitive UN-DATA avec «demande de confirmation non demandée».

La NLSPE qui invoque l'échange de commandes CSC doit attendre une primitive UN-DATA contenant une CSC PDU. Une primitive UN-RESET ou NLSP-RESET comme indiqué au 8.8 ou une primitive UN-DISCONNECT ou NLSP-DISCONNECT comme indiqué au 8.10 peut aussi avoir priorité sur l'échange de commandes CSC.

8.12.2 Primitive UN-DATA contenant une CSC PDU

A la réception d'une primitive UN-DATA contenant une CSC PDU (par l'entité appelante ou appelée dans le cadre d'un échange de commandes CSC), le contenu est vérifié conformément aux procédures spécifiques des mécanismes décrites au 10.3.

Selon les procédures spécifiques des mécanismes utilisées, la NLSPE peut:

a) renvoyer un contenu de CSC PDU et indiquer qu'un nouvel échange de commandes CSC est nécessaire,

auquel cas les marqueurs UNC-UND et SA-P de la CSC PDU doivent être libres, l'identificateur SA-ID doit être réglé à la valeur Your_SA-ID et le contenu doit être réglé conformément aux procédures spécifiques des mécanismes. La CSC PDU doit être envoyée dans le paramètre données d'utilisateur d'une primitive UN-DATA. La NLSPE doit attendre une autre primitive UN-DATA contenant une CSC PDU.

Une primitive UN-RESET ou NLSP-RESET comme indiqué au 8.8 ou une primitive UN-DISCONNECT ou NLSP-DISCONNECT comme indiqué au 8.10 peut aussi avoir priorité sur l'échange de commandes CSC;

b) renvoyer un contenu de CSC PDU et indiquer la SDT PDU nécessaire pour terminer l'échange,

auquel cas les marqueurs UNC-UND et SA-P de la CSC PDU doivent être libres, l'identificateur SA-ID doit être réglé à la valeur Your_SA-ID et le contenu doit être réglé conformément aux procédures spécifiques des mécanismes. La CSC PDU doit être envoyée dans le paramètre données d'utilisateur d'une primitive UN-DATA. La NLSPE doit attendre une autre primitive UN-DATA contenant une SDT PDU qui est traitée comme indiqué au 8.6. Une primitive UN-RESET ou NLSP-RESET comme indiqué au 8.8 ou une primitive UN-DISCONNECT ou NLSP-DISCONNECT comme indiqué au 8.10 peut aussi avoir priorité sur l'échange de commandes CSC;

NOTE 1 – L'authentification n'est pas jugée complète, donc les demandes NLSP-DATA (ou NLSP-EXPEDITED-DATA) ne doivent pas être traitées au niveau de cette NLSPE, tant qu'une SDT PDU n'a pas été reçue. Cette SDT PDU peut contenir un paramètre NLSP-DATA provenant de l'utilisateur NLSP distant ou peut n'être liée à aucune primitive de service NLSP.

NOTE 2 – Cette option ne peut être mise en œuvre si l'attribut No_Header est VRAI.

c) renvoyer un contenu de CSC PDU et indiquer que l'échange est terminé,

auquel cas les marqueurs UNC-UND et SA-P de la CSC PDU doivent être libres, l'identificateur SA-ID doit être réglé à la valeur Your_SA-ID et le contenu doit être réglé conformément aux procédures spécifiques des mécanismes. La CSC PDU doit être envoyée dans le paramètre données d'utilisateur d'une primitive UN-DATA;

d) indiquer qu'une SDT PDU doit être envoyée pour terminer l'échange de commandes CSC,

auquel cas, si la demande NLSP-DATA (ou NLSP-EXPEDITED-DATA) attend d'être envoyée et si l'attribut No_Header est FAUX, cette PDU doit être traitée comme indiqué au 8.6 ou 8.7. Dans le cas contraire, une SDT PDU doit être créée comme indiqué au 6.4.1.1, avec type de données «n'étant lié à aucune primitive de service NLSP» et ne contenant aucun champ de contenu autre que ceux généralement nécessaires au titre de l'article 6, et être envoyée dans le paramètre données d'utilisateur UN d'une primitive UN-DATA;

e) indiquer que l'échange de commandes CSC est terminé,

auquel cas aucune autre action n'est nécessaire.

NOTE 3 – Aucune procédure générale n'est définie pour résoudre les collisions entre deux échanges de commandes CSC déclenchés en même temps.

NOTE 4 – Avec les mécanismes d'authentification définis à l'article 10, si les fonctions d'encapsulation/de désencapsulation, telles que celles décrites à l'article 11, n'incluent pas l'utilisation de numéros ISN, l'authentification complète de l'entité homologue n'est pas assurée. L'authentification complète de l'entité homologue n'est pas non plus assurée si un mécanisme d'encapsulation fondé sur l'attribut No_Header, tel que celui décrit à l'article 12, est utilisé.

9 Vue d'ensemble des mécanismes utilisés

Les articles 9 à 12 définissent les mécanismes spécifiques qui doivent être utilisés avec le protocole générique défini aux articles 1 à 8. Ces mécanismes ne sont pas les seuls qui peuvent être utilisés pour assurer la sécurité dans le protocole NLSP générique. D'autres mécanismes pourront être normalisés dans le futur et il est possible d'utiliser des mécanismes privés avec le protocole NLSP.

9.1 Services et mécanismes de sécurité

Le protocole NLSP-CL permet de mettre en œuvre les services de sécurité suivants, s'ils sont sélectionnés, avec les mécanismes décrits:

a) *authentification de l'origine des données* – Le mécanisme utilisé pour assurer ce service est l'ICV (valeur de contrôle d'intégrité) conjointement avec la gestion de clés;

b) *contrôle d'accès* – Les mécanismes utilisés pour assurer ce service sont les étiquettes de sécurité et/ou la gestion de clés et/ou l'utilisation d'adresses authentifiées;

c) *confidentialité des données en mode sans connexion* – Le mécanisme utilisé pour assurer ce service est le codage. Cette protection inclut, à titre facultatif, tous les paramètres de service NLSP selon les services de sécurité sélectionnés;

d) *confidentialité du flux de trafic* – Le mécanisme utilisé pour assurer ce service est le remplissage de trafic et/ou la dissimulation de l'adresse NLSP;

e) *intégrité en mode sans connexion* – Le mécanisme utilisé pour assurer ce service est la valeur ICV. Cette protection inclut, à titre facultatif, tous les paramètres de service NLSP selon les services de sécurité sélectionnés.

Le protocole NLSP-CO permet de mettre en œuvre les services de sécurité suivants, s'ils sont sélectionnés, avec les mécanismes décrits:

a) *authentification de l'entité homologue* – Le mécanisme utilisé pour assurer ce service est un échange de numéros de séquence d'intégrité codés conjointement avec la gestion de clés;

b) *contrôle d'accès* – Les mécanismes utilisés pour assurer ce service sont les étiquettes de sécurité et/ou la gestion de clés et/ou les adresses authentifiées;

c) *confidentialité des données en mode connexion* – Le mécanisme utilisé pour assurer ce service est le codage. Cette protection inclut, à titre facultatif, tous les paramètres de connexion NLSP selon les services de sécurité sélectionnés;

d) *confidentialité du flux de trafic* – Le mécanisme utilisé pour assurer ce service est le remplissage de trafic et/ou la dissimulation de l'adresse;

e) *intégrité en mode connexion sans reprise* – Les mécanismes utilisés pour assurer ce service sont la valeur de contrôle d'intégrité (ICV) et les numéros de séquence d'intégrité (ISN). Cette protection inclut, à titre facultatif, tous les paramètres de connexion NLSP selon les services de sécurité sélectionnés.

9.2 Fonctions mises en œuvre

Les éléments essentiels des mécanismes mis en œuvre par le protocole NLSP sont les suivants:

a) une fonction d'authentification de connexion qui assure l'authentification de l'entité homologue et établit des valeurs initiales pour les attributs SA dynamiques servant de support au transfert de données sûres. Cette fonction est utilisée uniquement par le protocole NLSP-CO;

b) une fonction d'encapsulation fondée sur la SDT PDU qui assure le transfert de données sûres à l'aide des mécanismes suivants:

   1) numéro de séquence d'intégrité;

   2) remplissage pour la confidentialité du flux de trafic, algorithmes d'intégrité par bloc et algorithmes de codage par bloc;

   3) valeur de contrôle d'intégrité;

   4) codage;

c) une fonction d'encapsulation fondée sur la forme de protection avec attribut No_Header qui utilise un mécanisme de codage ne modifiant pas la longueur des données.

Les mécanismes sont mis en œuvre dans l'ordre indiqué ci-dessus.

10 Commande de sécurité de connexion (NLSP-CO seulement)

10.1 Vue d'ensemble

La procédure de «commande de sécurité de connexion» utilise un échange de PDU de commande de sécurité de connexion (CSC) pour:

a) spécifier, à titre facultatif, une nouvelle clé de codage/d'intégrité;

b) assurer l'authentification de l'entité homologue;

c) établir un numéro de séquence d'intégrité.

La mise en œuvre d'un mécanisme d'authentification fondé sur l'échange de numéros de séquence est spécifiée par la présente Recommandation | Norme internationale. L'authentification à l'aide de ce mécanisme est définitivement effectuée pour l'entité appelante lorsque l'échange bilatéral est terminé. Pour l'entité appelée, si la séquence d'intégrité est sélectionnée pour assurer la protection contre les attaques consistant à répéter des messages dans un but malveillant, (c'est-à-dire si l'attribut ISN est VRAI), l'authentification n'est définitivement effectuée qu'à la réception de la première SDT PDU de données ou de données de test provenant de l'entité appelante.

10.2 Attributs SA

Les attributs de sécurité suivants sont utilisés pour la mise en œuvre des procédures de commande de sécurité de connexion:

a) *Mécanismes sélectionnés pour l'association SA:*

Authentification: Valeur booléenne

Indique si l'authentification de l'entité homologue à l'aide du numéro ISN codé doit être utilisée.

Les valeurs de ces attributs sont définies par l'ASSR en fonction des services de sécurité sélectionnés.

b) *Attributs des mécanismes de répartition de clés:*

kdm: Mode à utiliser avec cette association SA

La valeur de cet attribut est définie par l'ASSR en fonction des services de sécurité sélectionnés.

Cet attribut peut avoir les valeurs suivantes:

kdm_mutual: répartition fondée sur des clés symétriques.

kdm_asymmetric_single: répartition fondée sur la clé publique du destinataire.

kdm_asymmetric_double: répartition fondée sur la clé publique distante et la clé privée locale.

kdm_distributed: répartition par référence à une clé préalablement répartie ou à une clé répartie par d'autres moyens.

kdm_other: un mécanisme de répartition défini à titre privé est utilisé.

c) *Attributs des mécanismes d'authentification:*

Auth_Alg: Identificateur d'objet attribué au titre de ISO/CEI 9979

La valeur de cet attribut est définie par l'ASSR en fonction des services de sécurité sélectionnés.

Enc_Auth_Len: Longueur du champ de données d'authentification codé dans la CSC PDU

La valeur de cet attribut est définie par l'ASSR en fonction des services de sécurité sélectionnés.

Auth_Gen_Key: Forme imposée par l'ASSR

La valeur initiale de cet attribut est fixée lors de l'établissement de l'association SA et peut être modifiée pendant la durée de l'association.

Auth_Check_Key: Forme imposée par l'ASSR

La valeur initiale de cet attribut est fixée lors de l'établissement de l'association SA et peut être modifiée pendant la durée de l'association.

Les attributs suivants utilisés par les mécanismes de transfert de données sûres peuvent être établis par le mécanisme d'authentification de connexion.

a) *Attributs de mécanisme ISN:*

Data_My_ISN

Data_Your_ISN

Exp_My_ISN

Exp_Your_ISN

b) *Attributs de mécanisme de codage:*

Data_Enc_Key

Data_Dec_Key

Exp_Enc_Key

Exp_Dec_Key

c) *Attributs de mécanisme ICV:*

Data_ICV_Gen_Key

Data_ICV_Check_Key

Exp_ICV_Gen_Key

Exp_ICV_Check_Key

NOTE – Des attributs additionnels spécifiques des mécanismes pourront être identifiés dans les futures versions de la présente Recommandation | Norme internationale, et pour des mécanismes privés.

10.3 Procédures

Les entités NLSP échangent des PDU de commande de sécurité de connexion (CSC) lors de chaque établissement de connexion ou à la suite d'une réinitialisation ou d'autres événements extérieurement programmés pour:

a) spécifier, à titre facultatif, la clé de codage ou d'intégrité;

b) assurer l'authentification de l'entité homologue;

c) établir un numéro de séquence d'intégrité.

L'authentification de l'entité homologue peut être assurée comme indiqué ci-dessous. Toute autre méthode doit fournir un numéro de séquence d'intégrité si l'intégrité de la connexion est nécessaire.

La clé de codage/d'intégrité est spécifiée:

a) par une indication que la clé existante doit être utilisée;

b) par transmission d'une nouvelle clé codée à l'aide d'une clé mutuelle de codage de clés;

c) par transmission d'une nouvelle clé codée à l'aide de la clé publique du destinataire;

d) par référence à une clé précédemment répartie.

NOTE 1 – Le calcul d'une clé de codage assure un certain niveau de contrôle d'intégrité car il empêche la répétition malveillante d'un texte codé protégé par une clé différente. L'algorithme de calcul de clé doit être spécifique de chaque algorithme de codage pour empêcher que des clés peu élaborées ne puissent être déterminées accidentellement par des tiers.

Le protocole NLSP utilise une méthode d'authentification de l'entité homologue fondée sur l'échange de numéros de séquence d'intégrité initiaux codés à l'aide d'une clé d'authentification. Cette méthode peut être mise en œuvre même si des numéros de séquence ne sont pas utilisés pour le service d'intégrité.

Les procédures de commande de sécurité de connexion sont fondées sur l'échange de deux CSC PDU et d'une PDU de transfert de données sûres comme suit.

Une CSC PDU est préparée par l'entité initiatrice de l'échange de sécurité, avec les éléments suivants:

a) attribut données d'authentification codées réglé à une valeur sélectionnée localement pour le champ My-Initial-ISN (mon numéro ISN initial) et à une valeur 0 pour le champ Your-Initial-ISN (votre numéro ISN initial) codés tous deux à l'aide de la clé Auth_Gen_Key. Le numéro ISN sélectionné doit être unique pour les clés d'authentification et d'intégrité;

b) informations de clé réglées conformément au mécanisme de répartition de clés.

A la réception d'une CSC PDU par une entité NLSP qui n'est pas déjà l'entité initiatrice d'un échange de CSC PDU:

a) l'attribut données d'authentification codées est décodé à l'aide de la clé Auth_Check_Key;

b) il convient de vérifier que le champ Your-Initial-ISN est égal à 0;

c) les attributs SA locaux Data_Your_ISN et Exp_Your_ISN sont réglés à la valeur du champ My-Initial-ISN reçu;

d) les informations de clé sont traitées conformément au mécanisme de répartition de clés.

Une CSC PDU est alors préparée avec:

a) l'attribut données d'authentification codées réglé à une valeur sélectionnée localement pour le champ My_Initial_ISN et à la valeur du champ My-Initial-ISN reçu pour le champ Your-Initial-ISN, tous deux codés à l'aide de la clé Auth_Gen_Key. Le numéro ISN sélectionné doit être unique pour les clés d'authentification et d'intégrité;

b) les informations de clé réglées conformément au mécanisme de répartition de clés.

A la réception d'une CSC PDU au niveau de l'entité initiatrice de l'échange de commandes CSC:

a) le paramètre données d'authentification codées est décodé à l'aide de la clé Auth_Check_Key;

b) il convient de vérifier le champ Your-Initial-ISN en fonction du champ My-Initial-ISN précédemment envoyé;

c) les attributs SA locaux Data_Your_ISN et Exp_Your_ISN sont réglés à la valeur du champ My-Initial-ISN reçu;

d) les informations de clé sont traitées conformément au mécanisme de répartition de clés.

Après vérification avec succès de la réponse, si l'entité NLSP n'a aucune donnée en attente et si le mécanisme ISN est sélectionné pour l'encapsulation de la SDT PDU (voir l'article 11), une PDU de transfert de données sûres ne contenant aucune donnée mais incluant un numéro ISN doit être envoyée pour mettre fin à l'authentification.

NOTE 2 – La SDT PDU peut être envoyée, même si aucune donnée n'est en attente pour terminer les procédures d'authentification, sans qu'il faille appliquer les procédures de transfert de données normales.

Si l'authentification échoue, l'association de sécurité peut, selon la décision prise localement, être réétablie dans la bande ou hors bande ainsi que par la mise en œuvre des procédures de reprise d'erreur décrites au 8.4.

10.4 Champs de CSC PDU utilisés

Les champs de contenu CSC suivants, spécifiques des mécanismes et définis au 13.5.6, sont utilisés dans le cadre des procédures décrites dans le présent paragraphe:

a) données d'authentification codées;

b) informations de clé.

11 Fonction d'encapsulation fondée sur la SDT PDU

11.1 Vue d’ensemble

Le protocole NLSP-CL et, à titre facultatif, le protocole NLSP-CO protègent les données d'utilisateur et les informations de commande de protocole connexes en utilisant une fonction d'encapsulation fondée sur la SDT PDU. Le présent paragraphe définit cette fonction d'encapsulation. Cette fonction d'encapsulation se subdivise en quatre fonctions:

– ISN;

– remplissage;

– ICV; et

– codage.

La décision d'employer une fonction particulière doit être fondée sur les attributs de l'association SA.

Si le numérotage de séquence est sélectionné, un champ ISN doit être ajouté.

NOTE 1 – L'utilisation de ce mécanisme de protection avec le protocole NLSP-CL n'est pas prévue.

Si le remplissage de trafic est sélectionné, un champ de remplissage de trafic peut être ajouté.

Si un algorithme d'intégrité par bloc est sélectionné, un champ de remplissage d'intégrité peut être ajouté.

Si le contrôle d'intégrité est sélectionné, une valeur ICV doit être calculée et ajoutée aux champs indiqués ci-dessus.

NOTE 2 – La valeur ICV peut être également utilisée pour assurer l'authentification de l'origine des données.

Si un algorithme de codage par bloc doit être utilisé, un champ de remplissage de codage peut être ajouté.

Si le codage est sélectionné, les champs indiqués ci-dessus sont codés à l'aide de la clé de codage pour l'association de sécurité.

La procédure décrite ci-dessus permet d'encapsuler les données d'utilisateur et d'autres paramètres de protocole NLSP pour assurer la protection de données lors de leur transfert dans un réseau. A l'extrémité distante, le destinataire d'une PDU de transfert de données sûres supprime et vérifie la protection en inversant l'ordre de la procédure.

11.2 Attributs SA

a) *Mécanismes sélectionnés pour l'association SA:*

ISN: Valeur booléenne

Numéros de séquence d'intégrité à inclure dans chaque champ Encapsulated-octet-string.

Padd: Valeur booléenne

Remplissage dans le champ Encapsulated-octet-string pour la mise en œuvre du mécanisme de remplissage de trafic.

ICV: Valeur booléenne

Authentification de l'intégrité et/ou de l'origine des données du champ Encapsulated-octet-string à l'aide d'une valeur de contrôle d'intégrité.

Encipher: Valeur booléenne

Codage d'un champ Encapsulated-octet-string pour assurer la confidentialité des données.

Les valeurs de ces attributs sont définies par l'ASSR en fonction des services de sécurité cibles sélectionnés.

b) *Attributs de mécanisme ISN:*

ISN_Len: Nombre entier

La valeur de cet attribut doit être définie par l'ASSR en fonction des services de sécurité sélectionnés.

Data_My_ISN: Numéro ISN pour les dernières données normales envoyées.

Data_Your_ISN: Numéro ISN pour les dernières données normales reçues.

Exp_My_ISN: Numéro ISN pour les dernières données exprès envoyées.

Exp_Your_ISN: Numéro ISN pour les dernières données exprès reçues.

La valeur initiale de ces attributs «clés» doit être fixée lors de l'établissement de l'association SA et peut être modifiée pendant la durée de l'association.

NOTE 1 – Les attributs ISN de données exprès ne sont applicables qu'au protocole NLSP-CO.

c) *Attributs de mécanisme de remplissage:*

Traff_Padd: Forme imposée par l'ASSR

Conditions requises pour le remplissage de trafic.

d) *Attributs de mécanisme ICV:*

ICV_Alg: Identificateur d'objet

La valeur de cet attribut doit être imposée par l'ASSR en fonction des services de sécurité sélectionnés. Cet attribut implique certains attributs de mécanisme d'intégrité tels que: algorithmes de génération et de vérification distincts, vecteurs d'initialisation, etc.

ICV_Blk: Nombre entier

Longueur de base d'un bloc traitée par l'algorithme ICV.

La valeur de cet attribut doit être imposée par l'ASSR en fonction des services de sécurité sélectionnés.

ICV_Len: Nombre entier

Longueur du résultat du mécanisme ICV.

La valeur de cet attribut doit être définie par l'ASSR en fonction des services de sécurité sélectionnés.

Il n'est pas nécessaire que l'attribut ICV_Len soit égal à l'attribut ICV_Blk.

Data_ICV_Gen_Key: Forme imposée par l'ASSR

Référence de clé de génération ICV pour les données normales.

Data_ICV_Check_Key: Forme imposée par l'ASSR

Référence de clé de vérification ICV pour les données normales.

Exp_ICV_Gen_Key: Forme imposée par l'ASSR

Référence de clé de génération ICV pour les données exprès.

Exp_ICV_Check_Key: Forme imposée par l'ASSR

Référence de clé de vérification ICV pour les données exprès.

La valeur initiale de ces attributs «clés» doit être fixée lors de l'établissement de l'association SA et peut être modifiée pendant la durée de l'association.

NOTE 2 – Les attributs de clés de données exprès ne sont applicables qu'au protocole NLSP-CO.

e) *Attributs de mécanisme de codage:*

Enc_Alg: Identificateur d'objet attribué conformément à ISO/CEI 9979

La valeur de cet attribut doit être imposée par l'ASSR en fonction des services de sécurité sélectionnés. Cet attribut implique certains attributs de mécanisme de codage tels que: forme et longueur de tout champ de synchronisation, algorithmes de codage et de décodage distincts, vecteurs d'initialisation, etc.

Enc_Blk: Nombre entier

Longueur d'un bloc d'algorithme de codage.

La valeur de cet attribut doit être imposée par l'ASSR en fonction des services de sécurité sélectionnés.

Data_Enc_Key: Forme imposée par l'ASSR

Référence de clé de codage pour les données normales.

Data_Dec_Key: Forme imposée par l'ASSR

Référence de clé de décodage pour les données normales.

Exp_Enc_Key: Forme imposée par l'ASSR

Référence de clé de codage pour les données exprès.

NOTE 3 – Cet attribut n'est utilisé que par le protocole NLSP-CO.

Exp_Dec_Key: Forme imposée par l'ASSR

Référence de clé de décodage pour les données exprès.

NOTE 4 – Cet attribut n'est utilisé que par le protocole NLSP-CO.

La valeur initiale des attributs «clés» doit être fixée lors de l'établissement de l'association SA et peut être modifiée pendant la durée de l'association.

NOTE 5 – Des attributs additionnels spécifiques des mécanismes pourront être identifiés dans les futures versions de la présente Recommandation | Norme internationale et pour des mécanismes privés.

11.3 Procédures

Lors de l'encapsulation, une PDU doit être formée par suffixation ou préfixation de champs. Ces champs peuvent être optionnels. Une PDU partiellement formée est désignée ci-après par le terme «champs existants». Lors de la désencapsulation, une PDU doit être décomposée par suppression des champs. Une PDU partiellement décomposée est désignée ci-après par le terme «données restantes».

NOTES

1 La description du mode de suffixation et de préfixation des champs n'a pas pour but de restreindre les possibilités de mise en œuvre du protocole NLSP mais plutôt de spécifier ce protocole sans ambiguïté.

2 La fonction d'encapsulation ne recouvre pas l'option No_Header. Cette option est traitée par les procédures définies à l'article 12.

11.3.1 Fonction d'encapsulation

L'identificateur SA-ID doit être utilisé pour désigner une association de sécurité. Si l'association de sécurité n'existe pas, l'erreur «SA-not-available» (SA non disponible) doit être renvoyée et la valeur du champ encapsulated-octet-string doit être indéterminée.

Si l'attribut ISN est VRAI:

a) si le type d'unité de données est «normal», l'attribut Data_Your_ISN doit être avancé, placé dans le champ de contenu numéro de séquence et ajouté aux champs existants dans le champ Octet-string-Before-Encapsulation;

b) si le type d'unité de données est «exprès», l'attribut Exp_Your_ISN doit être avancé, placé dans le champ de contenu numéro de séquence et ajouté aux champs existants dans le champ Octet-string-Before-Encapsulation.

NOTES

1 Le numéro ISN peut être avancé par incrémentation d'un numéro de séquence ou par le choix du numéro suivant dans une séquence non répétitive. Des timbres horodateurs peuvent être également considérés comme une séquence non répétitive.

2 L'utilisation du mécanisme ISN avec le protocole NLSP-CL n'est pas prévue.

3 L'attribut Exp_My_ISN n'est applicable qu'au protocole NLSP-CO.

Si l'attribut Padd est VRAI, un remplissage, dont la longueur et la forme sont déterminées localement par les règles de l'ASSR auxquelles il est fait référence dans l'attribut Traff_Padd, doit être placé dans un champ de contenu remplissage de trafic et ajouté après les champs existants dans le champ Octet-String-Before-Encapsulation. Si un seul octet de remplissage est nécessaire, il convient d'utiliser le champ de contenu remplissage à un seul octet.

Si l'attribut ICV est VRAI et si l'attribut ICV_Blk est supérieur à 1, un champ de remplissage d'intégrité doit, s'il y a lieu, être ajouté après les champs existants de telle sorte que la longueur des champs existants avec le champ de remplissage d'intégrité (y compris le champ de contenu protégé), soit un nombre entier multiple de la longueur du bloc ICV (c'est-à-dire de l'attribut ICV_Blk). Si ce champ est présent, un remplissage, dont la longueur et la forme sont déterminées localement, doit être placé dans un champ de contenu remplissage d'intégrité. Si un seul octet de remplissage est nécessaire, le champ de contenu remplissage à un seul octet doit être utilisé. La valeur de la longueur du contenu doit être augmentée de la longueur de remplissage ajoutée.

Un champ longueur de contenu doit être placé avant les champs existants. La longueur de tous les champs existants doit être déterminée et placée dans ce champ longueur de contenu.

Si l'attribut ICV est VRAI, une valeur ICV de longueur ICV_Len doit être calculée et ajoutée après les champs existants. L'algorithme utilisé doit être identifié par l'attribut ICV_Alg et la clé utilisée doit être:

a) Data_ICV_Gen_Key si le type d'unité de données est normal, ou

b) Exp_ICV_Gen_Key si le type d'unité de données est exprès.

Si l'attribut Encipher est VRAI, un champ de synchronisation cryptographique ayant une forme et une longueur déterminées par l'attribut Enc_Alg doit être créé et ajouté avant les champs existants.

Si l'attribut Encipher est VRAI, un remplissage de codage doit être ajouté après les champs existants de telle sorte que la longueur de ceux-ci (c'est-à-dire les champs Protected Data Length, Octet-String-Before-Encapsulation, ISN, Integrity Pad et ICV), plus la longueur du remplissage de codage, soit un nombre entier multiple de la longueur d'un bloc de codage (c'est-à-dire Enc_Blk). S'il est présent, le remplissage, dont la longueur et la forme sont déterminées localement, doit être placé dans un champ de contenu remplissage de codage. Si un seul octet de remplissage est nécessaire, le champ de contenu remplissage à un seul octet doit être utilisé.

Si l'attribut Encipher est VRAI, les champs existants sont codés. L'algorithme utilisé doit être identifié par l'attribut Enc_Alg et la clé utilisée doit être:

a) Data_Enc_Key si le type d'unité de données est normal, ou

b) Exp_Enc_Key si le type d'unité de données est exprès.

La PDU construite qui en résulte doit être renvoyée dans le champ encapsulated-octet-string.

11.3.2 Fonction de désencapsulation

Si l'une quelconque des vérifications suivantes échoue, toutes les informations d'état relatives à la sécurité seront réglées à la valeur informations d'état relatives à la sécurité avant réception de ce message, sauf pour les informations d'alarme, d'audit et/ou de comptabilité.

L'argument SA-ID doit être utilisé pour désigner une association de sécurité. Si l'association de sécurité n'existe pas, l'erreur «SA-not-available» (SA non disponible) doit être renvoyée et la valeur du champ Octet-String-Before-Encapsulation doit être indéterminée.

Si l'attribut Encipher est VRAI, les actions suivantes sont entreprises:

a) Le champ encapsulated-octet-string doit être décodé. L'algorithme de décodage utilisé doit être identifié par l'attribut Enc_Alg et la clé utilisée doit être:

   1) Data_Dec_Key si le type d'unité de données est normal, ou

   2) Exp_Dec_Key si le type d'unité de données est exprès.

b) Il convient de supprimer le champ de synchronisation cryptographique en éliminant, conformément à l'attribut Enc_Alg, un certain nombre d'octets de la partie avant des données codées.

c) Il convient de supprimer le remplissage de codage ou le champ de contenu remplissage à un seul octet en ajoutant la longueur de contenu et l'attribut ICV_Len puis en éliminant, dans les données codées restantes, tout octet au-delà de la longueur calculée.

Si l'attribut ICV est VRAI, les actions suivantes sont entreprises:

a) Il convient de vérifier le champ ICV en contrôlant les derniers octets ICV-Len des données restantes. L'algorithme utilisé doit être identifié par l'attribut ICV_Alg et, s'il est fondé sur un mécanisme cryptographique, la clé utilisée pour calculer la valeur ICV doit être:

   1) Data_ICV_Check_Key si le type d'unité de données est normal, ou

   2) Exp_ICV_Check_Key si le type d'unité de données est exprès.

b) Si la vérification ICV échoue, l'erreur data-unit-integrity-failure (échec d'intégrité d'unité de données) doit être renvoyée et la valeur du champ Octet-String-Before-Encapsulation doit être indéterminée.

Il convient de supprimer la valeur ICV en éliminant, dans les données restantes, tout octet au-delà de la longueur contenue dans le paramètre longueur de contenu après le champ longueur de contenu.

Il convient de supprimer le champ longueur de contenu en éliminant les deux premiers octets des données restantes.

Il convient de supprimer des données restantes tout champ de contenu remplissage de trafic, remplissage d'intégrité ou remplissage à un seul octet en éliminant les données au-delà du champ Octet-String-Before-Encapsulation.

NOTE 1 – On localise les champs de contenu en décodant le contenu du champ Octet-String-Before-Encapsulation qui est un champ de type à un octet suivi d'un certain nombre de champs TLV.

Si l'attribut ISN est VRAI, il convient de vérifier les données restantes pour s'assurer qu'un seul et unique champ de contenu ISN est présent; sinon, il convient de vérifier les données restantes pour s'assurer qu'aucun champ de contenu ISN n'est présent. Si ce champ est présent, il convient de vérifier que la valeur du numéro ISN est:

a) si on a (data_unit_type = normal), l'attribut Data_My_ISN est avancé dans sa fenêtre et la valeur ainsi reçue est comparée à la fenêtre des valeurs attendues selon cet attribut;

b) si on a (data_unit_type = expedited), l'attribut Exp_My_ISN est avancé et la valeur ainsi reçue dans sa fenêtre est comparée à la fenêtre des valeurs attendues selon cet attribut.

Dans les deux cas a) et b), l'attribut ISN est avancé avant la vérification.

NOTE 2 – L'avancement peut être effectué par incrémentation d'un numéro de séquence ou par le choix du numéro suivant dans une séquence pseudo-aléatoire, non répétitive.

La valeur du champ Octet-String-Before-Encapsulation qui en résulte doit être renvoyée dans le champ Octet-String-Before-Encapsulation.

11.4 Champs de PDU utilisés

Ces procédures utilisent les champs suivants d'une SDT PDU tels que définis au 13.3:

a) Encapsulated-Octet-String (chaîne d'octets encapsulée);

b) Synchronisation cryptographique;

c) ICV;

d) Champs de contenu:

   1) remplissage de codage;

   2) numéro de séquence;

   3) remplissage à un seul octet;

   4) remplissage de trafic;

   5) remplissage d'intégrité.

12 Fonction d'encapsulation fondée sur l'attribut No_Header (NLSP-CO seulement)

12.1 Vue d'ensemble

Le protocole NLSP-CO ne peut assurer la confidentialité des données d'utilisateur qu'à l'aide de l'option No_Header qui utilise une fonction d'encapsulation telle que celle décrite dans le présent paragraphe. Cette fonction d'encapsulation doit être fondée sur un mécanisme de codage.

L'utilisation de l'option No_Header implique que le mécanisme de codage traite un bloc d'une longueur d'un octet et que l'algorithme ne modifie pas la longueur des données codées.

12.2 Attributs SA

a) Mécanismes sélectionnés pour l'association SA:

Encipher: Valeur booléenne

Codage d'un champ encapsulated-octet-string pour assurer la confidentialité des données.

Les valeurs de cet attribut doivent être définies par l'ASSR en fonction des services de sécurité sélectionnés.

b) Attributs de mécanisme de codage:

Enc_Alg: Identificateur d'objet attribué conformément à ISO/CEI 9979

La valeur de cet attribut doit être définie par l'ASSR en fonction des services de sécurité sélectionnés. Cet attribut implique certains attributs de mécanisme de codage tels que: forme et longueur de tout champ de synchronisation, algorithmes de codage et de décodage distincts, vecteurs d'initialisation, etc.

Data_Enc_Key: Forme imposée par l'ASSR

Référence de clé de codage pour les données normales.

Data_Dec_Key: Forme imposée par l'ASSR

Référence de clé de décodage pour les données normales.

Exp_Enc_Key: Forme imposée par l'ASSR

Référence de clé de codage pour les données exprès.

Exp_Dec_Key: Forme imposée par l'ASSR

Référence de clé de décodage pour les données exprès.

La valeur initiale de ces attributs «clés» doit être fixée lors de l'établissement de l'association SA et peut être modifiée pendant la durée de l'association.

NOTE – Des attributs additionnels, spécifiques des mécanismes, pourront être identifiés dans les futures versions de la présente Recommandation | Norme internationale et pour des mécanismes privés.

12.3 Procédures

12.3.1 Fonction d'encapsulation

L'identificateur SA-ID est utilisé pour désigner une association de sécurité. Si l'association de sécurité n'existe pas, l'erreur SA-not-available (SA non disponible) doit être renvoyée et la valeur du champ encapsulated-octet-string doit être indéterminée.

Si l'attribut Encipher est VRAI, le champ Octet-String-Before-Encapsulation doit être codé. L'algorithme utilisé doit être identifié par l'attribut Enc_Alg et la clé utilisée doit être:

a) Data_Enc_Key si le type d'unité de données est normal, ou

b) Exp_Enc_Key si le type d'unité de données est exprès.

Les données codées qui en résultent doivent être renvoyées dans le champ encapsulated-octet-string.

12.3.2 Fonction de désencapsulation

Si l'une quelconque des vérifications échoue, toutes les informations d'état relatives à la sécurité seront réglées à la valeur informations d'état relatives à la sécurité avant réception de ce message, sauf pour les informations d'alarme, d'audit et/ou de comptabilité.

L'argument SA-ID doit être utilisé pour désigner une association de sécurité. Si l'association de sécurité n'existe pas, l'erreur SA-not-available (SA non disponible) doit être renvoyée et la valeur du champ Octet-String-Before-Encapsulation doit être indéterminée.

Si l'attribut Encipher est VRAI, le champ encapsulated-octet-string doit être décodé. L'algorithme de décodage utilisé doit être identifié par l'attribut Enc_Alg et la clé utilisée doit être:

a) Data_Dec_Key si le type d'unité de données est normal, ou

b) Exp_Dec_Key si le type d'unité de données est exprès.

La valeur des données codées qui en résulte doit être renvoyée dans le champ Octet-String-Before-Encapsulation.

13 Structure et codage des PDU

13.1 Introduction

Le protocole NLSP utilise 3 types de PDU:

a) PDU de transfert de données sûres;

b) PDU d'association de sécurité;

c) PDU de commande de sécurité de connexion.

Un autre format de données non structuré sans informations PCI est utilisé avec l'option No_Header pour les données protégées.

Toutes les PDU doivent contenir un nombre entier d'octets. Les octets dans une PDU sont numérotés à partir de un (1) et augmentent dans l'ordre où ils sont placés dans la demande du «réseau de base» appropriée. Lorsque des octets consécutifs sont utilisés pour représenter un nombre binaire, le nombre ayant le moins d'octets a la valeur la plus significative. Les bits dans un octet sont numérotés de un (1) à huit (8) mais le bit un (1) est le bit d'ordre inférieur.

Lorsque le codage d'une PDU est représenté à l'aide d'un diagramme dans le présent paragraphe:

a) les octets sont indiqués avec, à gauche ou au-dessus, l'octet dont le numéro est le plus faible;

b) dans un octet, les bits sont indiqués avec le bit huit (8) à gauche et le bit un (1) à droite.

Les notations au-dessous d'une case indiquent la longueur de chaque champ en octets: l'abréviation «var» indique que la longueur de champ est variable.

La présence ou l'absence d'un champ «optionnel» doit être spécifiée par les attributs contenus dans l'association de sécurité.

NOTE – Les champs optionnels sont ainsi appelés parce qu'une association de sécurité donnée nécessite la présence de certains champs et l'absence d'autres champs. Une fois que l'association de sécurité est décidée, la présence ou l'absence de chaque champ est déterminée par les attributs SA.

13.2 Format du champ de contenu

Le champ de contenu est un format de champ général pour les valeurs de données à placer dans les PDU définies dans le présent paragraphe (voir la Figure 13-1).

Type	Longueur	Valeur
1	1-3	var

Figure 13-1 – Champ de contenu

Le type de champ de contenu doit être réglé à l'une des valeurs suivantes:

Valeur	*Type de champ de contenu*
00-5F	Réservé pour utilisation privée
60-9F	Réservé pour utilisation future
A0-BF	Réservé pour utilisation de SA-P (voir l'Annexe C)
C0-CF	Réservé pour utilisation indépendante des mécanismes (voir 13.3.4.3)
D0-FF	Réservé pour utilisation indépendante des mécanismes (voir 13.3.5)

La longueur de champ de contenu doit contenir la longueur de la valeur du champ de contenu en octets. La longueur du champ de contenu doit être de un, deux ou trois octets:

a) si elle est d'un octet, le bit 8 doit être égal à 0 et les 7 autres bits définissent une longueur de champ allant jusqu'à 127 octets;

b) si elle est de deux octets, le premier octet doit être codé sous la forme 1000 0001 et l'autre octet définit une longueur de champ allant jusqu'à 255 octets;

c) si elle est de trois octets, le premier octet doit être codé sous la forme 1000 0010 et les 2 autres octets définissent une longueur de champ allant jusqu'à 65 535 octets.

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

La valeur du champ de contenu doit contenir des données pour le champ de PDU.

13.3 Données protégées

Le présent paragraphe définit les PDU utilisées pour le transfert de données protégées. Cette définition porte notamment sur deux aspects des PDU, à savoir celles qui sont indépendantes des mécanismes utilisés (désignées par le terme «génériques») et celles qui sont spécifiques des mécanismes mis en œuvre par les procédures d'encapsulation définies à l'article 11 (désignées par le terme «spécifiques des mécanismes»). Celles qui comportent les aspects à la fois génériques et spécifiques des mécanismes sont désignées par le terme mixtes.

13.3.1 Structures de base des PDU (génériques)

Deux structures de données sont définies pour le transfert de données sûres. La première est obligatoire pour le protocole NLSP-CL; l'une des deux doit être mise en œuvre pour le protocole NLSP-CO.

a) PDU de transfert de données sûres formatée comme indiqué sur la Figure 13-2.

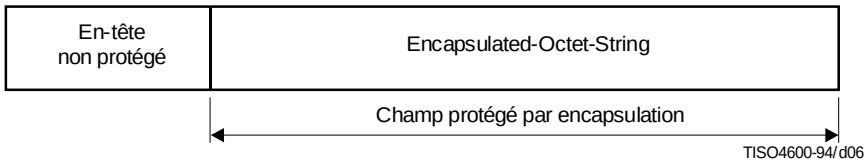


Figure 13-2 – Structure d'une PDU générique de transfert de données sûres

La structure de l'en-tête non protégé est définie au 13.3.2. Le champ Encapsulated-Octet-String doit contenir le résultat d'une fonction d'encapsulation (par exemple, comme indiqué à l'article 11 et obtenu à l'aide de la structure définie au 13.3.3) appliquée au champ Octet-String-Before-Encapsulation structuré comme indiqué au 13.3.4.

Les conditions (obligatoire/facultatif, etc.) de mise en œuvre des champs formant cette PDU sont définies dans D.5.3, D.5.4 (champs spécifiques des mécanismes), D.6.4 (NLSP-CL seulement) et D.7.6 (NLSP-CO seulement).

b) Chaîne binaire non structurée pour l'option confidentialité en mode No_Header seulement formatée comme indiqué sur la Figure 13-3. Aucune information PCI n'est ajoutée.

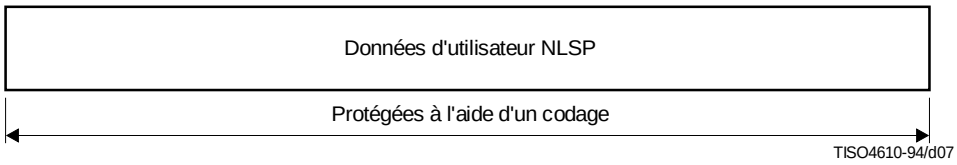


Figure 13-3 – Confidentialité utilisant uniquement l'option No_Header

L'option No_Header doit être utilisée uniquement lorsque toutes les conditions suivantes sont satisfaites:

a) l'attribut No_Header est VRAI;

b) l'attribut Label est FAUX;

c) l'attribut ICV est FAUX;

d) l'attribut ISN est FAUX;

e) l'attribut Encipher est VRAI;

f) l'attribut Enc_Sync_Len = 0;

g) l'attribut Enc_Blk = 1;

h) l'attribut Pad est FAUX.

13.3.2 En-tête non protégé (générique)

Le format de l'en-tête non protégé doit être celui indiqué sur la Figure 13-4.

Id de protocole	LI	Type de PDU	SA-ID
1	1	1	var

Figure 13-4 – En-tête non protégé

13.3.2.1 Id de protocole (générique)

Ce champ doit contenir l'identificateur de protocole NLSP, valeur 1000 1011.

13.3.2.2 LI (générique)

Ce champ doit contenir la longueur du champ de type de PDU plus l'identificateur SA-ID.

Pour le protocole NLSP-CO, le champ SA-ID n'est pas nécessaire. Ce champ doit donc être réglé de telle sorte que le champ SA-ID ne soit pas présent (c'est-à-dire à la valeur 00000001).

13.3.2.3 Type de PDU (générique)

Ce champ doit contenir le type de PDU, valeur 0100 1000 pour indiquer une PDU de transfert de données sûres.

13.3.2.4 SA-ID (générique)

Le champ SA-ID doit contenir l'identificateur d'association de sécurité de l'entité distante (c'est-à-dire l'attribut SA Your_SA-ID). Ce champ n'est pas nécessaire pour le protocole NLSP-CO.

13.3.3 Encapsulated-Octet-String (spécifique des mécanismes)

La structure de la SDT PDU qui utilise les procédures spécifiques des mécanismes définies à l'article 13 doit être celle indiquée sur la Figure 13-5.

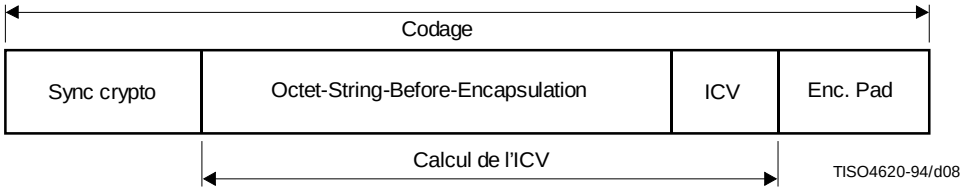


Figure 13-5 – Structure du champ Encapsulated-Octet-String

13.3.3.1 Synchronisation cryptographique (spécifique des mécanismes)

Il s'agit d'un champ optionnel qui peut contenir des données de synchronisation pour des algorithmes de codage spécifiques. Sa présence, sa forme et sa longueur résultent implicitement de l'attribut Enc_Alg.

13.3.3.2 Valeur de contrôle d'intégrité (spécifique des mécanismes)

Ce champ contient une valeur de contrôle d'intégrité (ICV). La longueur de ce champ doit être définie par l'identificateur d'algorithme d'ICV contenu dans les attributs d'association de sécurité.

13.3.3.3 Remplissage de codage (spécifique des mécanismes)

Ce champ contient un remplissage de codage (Enc_Pad) pour la mise en œuvre d'algorithmes de codage par bloc assurant la confidentialité des données. Le choix de la valeur de remplissage relève du domaine local. Toutes les NLSPE doivent pouvoir rejeter ce champ. Le format de ce champ doit être codé comme indiqué au 13.2 ou conformément à l'algorithme de codage. Le code de type de ce champ TLV doit être celui indiqué au 13.3.5. Si un remplissage à deux octets est nécessaire, la longueur doit être égale à zéro sans aucune valeur. Si un remplissage à un seul octet est nécessaire, un champ «remplissage à un seul octet» doit être utilisé au lieu d'un champ «remplissage de codage».

Ce champ n'est utilisé que si l'algorithme de codage nécessite un remplissage de codage indépendant.

13.3.4 Champ Octet-String-Before-Encapsulation (mixte)

La Figure 13-6 indique le format du champ Octet-String-Before-Encapsulation. Ce champ contient un nombre quelconque de champs de contenu génériques et spécifiques des mécanismes.

Au moins la longueur de contenu et le type de données doivent être présents.

Longueur de contenu	Type de données	Champ de contenu (générique)	. .	Champ de contenu spécifique des mécanismes	. .
2	1	var		var	

Figure 13-6 – Champ Octet-String-Before-Encapsulation

13.3.4.1 Longueur de contenu (générique)

Ce champ doit contenir la longueur combinée de tous les champs de contenu et du type de données.

NOTE – Ce champ ne comprend pas les champs ICV ou remplissage de codage.

13.3.4.2 Type de données (générique)

Le bit 8 de ce champ doit être le marqueur «entité appelante vers entité appelée». Une valeur de 1 indique entité appelante vers entité appelée. Une valeur de 0 indique entité appelée vers entité appelante.

Le bit 7 de ce champ doit être le marqueur «Last/Not last» (champ complet/champ partiel). Ce bit doit prendre la valeur 0 lorsque la SDT PDU contient le dernier segment d'une séquence. Dans le cas contraire, il doit prendre la valeur 1. Dans le cas du protocole NLSP en mode sans connexion, ce bit doit toujours être à la valeur 0.

Les bits 1 à 6 de ce champ sont codés pour identifier les primitives de service NLSP comme suit:

Valeur	*Primitive de service*
000000	Bit n'étant lié à aucune primitive de service NLSP (par exemple, données de test)
000001	dem./ind. NLSP-UNITDATA
000010	dem./ind. NLSP-CONNECT
000011	rép./conf. NLSP-CONNECT
000100	dem./ind. NLSP-DATA
000101	dem./ind. NLSP-DATA-ACKNOWLEDGE
000110	dem./ind. NLSP-EXPEDITED-DATA
000111	dem./ind. NLSP-DISCONNECT
001000	Protocole SA
001001-011111	Réservé pour utilisation future
100000-111111	Réservé pour utilisation privée

13.3.4.3 Champs de contenu (génériques)

Le codage du type de champ de contenu doit être celui défini au 13.2. Les champs de contenu indépendants des mécanismes (c'est-à-dire C0-CF) utilisés par les procédures des articles 6, 7 et 8 sont indiqués ci-dessous:

Valeur	*Type de champ de contenu*
00-BF	Réservé
C0	Données d'utilisateur
C1	Données de test
C2	Adresse NLSP appelante/d'origine
C3	Adresse NLSP appelée/de destination
C4	Adresse NLSP répondante
C5	Non utilisé
C6	Etiquette
C7	Référence d'étiquette
C8	Demande de confirmation
C9	Raison de la déconnexion
CA-CF	Réservé pour utilisation future
D0-FF	Réservé

13.3.4.3.1 Données d'utilisateur NLSP

Ce champ contient les données d'utilisateur NLSP de la primitive de service.

13.3.4.3.2 Données de test

La structure des données de test est indiquée sur la Figure 13-7.

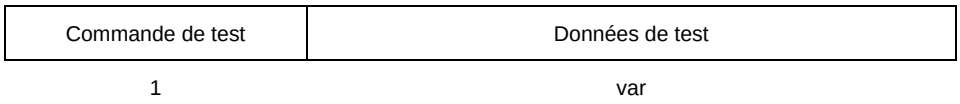


Figure 13-7 – Données de test

La commande de test contient une série de bits attribués comme suit:

a) bit 1 – Marqueur de direction, 0 pour données de test initiales, 1 pour données de test réfléchies;

b) bits 2 à 4 – Réservés pour utilisation future;

c) bits 5 à 8 – Réservés pour utilisation privée.

13.3.4.3.3 Adresse NLSP appelante/d'origine

Ce champ contient une adresse de couche réseau codée sous l'une des formes décrites dans la Rec. X.213 du CCITT | ISO 8348/AD2.

13.3.4.3.4 Adresse NLSP appelée/de destination

Ce champ contient une adresse de couche réseau codée sous l'une des formes décrites dans la Rec. X.213 du CCITT | ISO 8348/AD2.

13.3.4.3.5 Adresse NLSP répondante

Ce champ contient une adresse de couche réseau codée sous l'une des formes décrites dans la Rec. X.213 du CCITT | ISO 8348/AD2.

13.3.4.3.6 Etiquette

Ce champ est utilisé pour acheminer l'étiquette de sécurité d'une PDU. Il n'est pas présent si un champ de contenu de référence d'étiquette est présent (voir la Figure 13-8).

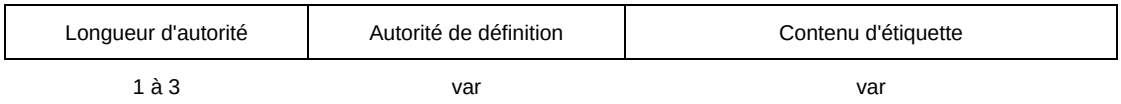


Figure 13-8 – Valeur d'étiquette

L'autorité de définition doit être codée sous la forme du contenu d'une valeur d'identificateur d'objet et à l'aide des règles de codage de base d'un identificateur d'objet défini dans la Rec. X.209 du CCITT | ISO 8825, article 22.

La structure et l'interprétation du contenu de l'étiquette sont définies par diverses autorités de définition.

NOTE – Il est prévu que ces étiquettes seront enregistrées conformément aux procédures définies par l'UIT-T/l'ISO/CEI. Une autorité de définition sera enregistrée comme un identificateur d'objet à l'aide des procédures définies dans ISO/CEI 9834.

13.3.4.3.7 Référence d'étiquette

Ce champ identifie l'une des étiquettes de sécurité de l'ensemble défini dans l'attribut SA Label_Set. Lorsqu'il est présent, ce champ doit toujours être codé de telle sorte que la partie valeur du champ soit de deux octets. Ce champ ne doit pas être présent si un champ de contenu d'étiquette est présent.

13.3.4.3.8 Demande de confirmation

Lorsqu'il est présent, ce champ indique que la confirmation de réception est demandée. Ce champ doit être codé sous la forme d'un code de type à un octet (sans longueur ni valeur).

13.3.4.3.9 Raison de la déconnexion

Ce champ doit acheminer le paramètre de service NLSP-DISCONNECT reason (raison de la déconnexion NLSP) codé tel que lorsqu'il est acheminé dans le réseau de base.

NOTE – Dans le cas où le réseau de base est un réseau conforme à la Rec. X.25 du CCITT | ISO 8208, le premier octet est la valeur de la cause et, s'il est présent, le second octet est le code de diagnostic correspondant à la raison NLSP-DISCONNECT définie dans la Rec. X.223 du CCITT | ISO 8878.

13.3.5 Champs de contenu (spécifiques des mécanismes)

Le codage du champ de contenu doit être celui défini au 13.2. Le codage du type de champ de contenu pour les champs de contenu spécifiques des mécanismes est indiqué ci-dessous:

Valeur	*Type de champ de contenu*
00-CF	Réservé
D0	Numéro de séquence
D1	Remplissage à un seul octet
D2	Remplissage de trafic
D3	Remplissage d'intégrité
D4	Remplissage de codage
D5-FF	Réservé pour utilisation future

13.3.5.1 Numéro de séquence

Ce champ contient l'attribut Your_ISN (c'est-à-dire un numéro de séquence d'intégrité de PDU) qui doit être unique compte tenu de la clé en vigueur pour ce type de données (exprès ou normal).

NOTE – Dans le protocole NLSP-CO, l'unicité entre les flux de données exprès et normales (donc la protection contre les répétitions malveillantes de messages) est assurée par l'utilisation d'un champ de type de données différent (voir 13.3.4.2).

13.3.5.2 Remplissage à un seul octet

Ce champ doit être un champ de type à un octet (sans longueur ni valeur) pour le remplissage générique (par exemple, pour la mise en œuvre d'un remplissage d'intégrité à un seul octet). Cet octet peut être utilisé une ou plusieurs fois au lieu d'un champ de remplissage d'intégrité, de codage ou de données codé TLV, pour assurer le remplissage d'intégrité, de codage ou de trafic. Toutes les NLSPE doivent pouvoir détecter et rejeter ce champ.

13.3.5.3 Remplissage de trafic

Ce champ contient un remplissage visant à assurer la confidentialité du flux de trafic. Le choix de la valeur de remplissage relève du domaine local. Toutes les NLSPE doivent pouvoir détecter et rejeter ce champ. Si un remplissage à deux octets est nécessaire, la longueur doit être égale à zéro et sans valeur. Si un remplissage à un seul octet est nécessaire, un champ remplissage à un seul octet doit être utilisé au lieu d'un champ remplissage de trafic.

13.3.5.4 Remplissage d'intégrité

Ce champ contient un remplissage pour la mise en œuvre d'algorithmes d'intégrité par bloc. Le choix de la valeur de remplissage relève du domaine local. Toutes les NLSPE doivent pouvoir rejeter ce champ. Si un remplissage à deux octets est nécessaire, la longueur doit être égale à zéro et sans valeur. Si un remplissage à un seul octet est nécessaire, un champ remplissage à un seul octet doit être utilisé au lieu d'un champ remplissage d'intégrité.

Ce champ peut être également utilisé pour répondre aux besoins du remplissage de codage.

13.4 PDU d'association de sécurité

Le format de la PDU d'association de sécurité doit être celui indiqué sur la Figure 13-9.

Les conditions (obligatoire/facultatif, etc.) pour la mise en œuvre des champs formant cette PDU sont définies dans D.5.5 et D.5.6 (champs spécifiques des mécanismes).

Id de protocole	LI	Type de PDU	SA-ID	Type de SA-P	Contenu de la SA PDU
1	1	1	var	1	var

Figure 13-9 – Structure de la PDU d'association de sécurité

13.4.1 Identificateur de protocole (PID)

Ce champ contient l'identificateur de protocole NLSP, valeur 10001011.

13.4.2 LI

Ce champ contient la longueur du champ de type d'unité PDU plus le champ SA-ID.

Si le protocole SA-P doit signaler qu'il ne connaît pas l'identificateur SA-ID de son entité homologue (par exemple, lors de l'établissement d'une nouvelle association SA), ce champ doit être réglé à la valeur 00000001 pour indiquer que le champ SA-ID n'est pas présent.

13.4.3 Type de PDU

Ce champ doit contenir la valeur de type de PDU 01001001 pour indiquer une PDU d'association de sécurité.

13.4.4 SA-ID

Le champ SA-ID doit contenir l'identificateur d'association de sécurité de l'entité distante (c'est-à-dire l'attribut SA Your_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).

13.4.5 Type de SA-P

Ce champ doit contenir un identificateur d'objet indiquant le mécanisme utilisé pour mettre en œuvre le protocole SA. Cet identificateur d'objet doit être codé sous la forme du contenu d'une valeur d'identificateur d'objet et à l'aide des règles de codage de base définies dans la Rec. X.209 du CCITT | ISO/CEI 8825, article 22.

L'identificateur d'objet indiqué ci-dessous est assigné pour l'utilisation du protocole SA-P générique avec les procédures d'échange de jetons de clé définies dans l'Annexe C ainsi qu'avec l'algorithme d'échange de clés exponentielles décrit dans l'Annexe H:

joint-ccitt-iso nlsp (22) sa-p-kte (1) eke (1)

L'utilisation d'autres protocoles SA ou algorithmes avec le protocole SA-P défini dans l'Annexe C peut être indiquée par d'autres identificateurs d'objet attribués conformément à ISO/CEI 9834-1.

13.4.6 Contenu de la SA PDU

La structure interne de ce champ dépend du mécanisme de mise en œuvre du protocole SA comme spécifié au 13.4.5 ci-dessus. L'Annexe C définit l'un de ces protocoles SA.

13.5 PDU de commande de sécurité de connexion

Le format de la PDU de commande de sécurité de connexion doit être celui indiqué sur la Figure 13-10.

Les conditions (obligatoire/facultatif, etc.) de mise en œuvre des champs formant cette PDU sont définies dans D.7.7 et D.7.8 (champs spécifiques des mécanismes).

Id de protocole	LI	Type de PDU	SA-ID	Longueur du contenu	Contenu de la CSC PDU
1	1	1	var	1	var

Figure 13-10 – PDU de commande de sécurité de connexion

13.5.1 Identificateur de protocole

Ce champ doit contenir l'identificateur de protocole NLSP, valeur 10001011.

13.5.2 LI

Ce champ doit contenir la longueur du champ de type de PDU plus le champ SA-ID.

13.5.3 Type de PDU

Ce champ doit contenir la valeur de type de PDU xx111111 pour indiquer une PDU de commande de sécurité de connexion. Les valeurs de bit pour ce champ doivent être les suivantes:

a) les bits 1 à 6 doivent contenir la valeur de type de PDU 111111 pour indiquer une PDU de commande de sécurité de connexion;

b) le bit 7 – Marqueur UNC-UND, s'il est positionné, doit indiquer que le paramètre NLSP-CONNECT est acheminé dans une primitive UN-DATA; dans le cas contraire, s'il est libre, il doit indiquer que le paramètre NLSP-CONNECT est acheminé dans une primitive UN-CONNECT;

c) le bit 8 – Marqueur SA-P, doit indiquer que le protocole SA-P est invoqué dans cette connexion. Si ce bit est positionné, aucun autre champ n'est présent dans cette PDU.

13.5.4 SA-ID

Le champ SA-ID doit contenir l'identificateur d'association de sécurité de l'entité distante (c'est-à-dire l'attribut SA Your_SA-ID). Ce champ ne doit pas être présent si le marqueur SA-P est positionné.

13.5.5 Longueur de contenu

Ce champ doit contenir la longueur du contenu de la CSC PDU en octets. Ce champ ne doit pas être présent si le marqueur SA-P est positionné.

13.5.6 Contenu de CSC PDU

La structure interne de ce champ dépend du mécanisme de mise en œuvre de l'authentification de connexion. Ce champ ne doit pas être présent si le marqueur SA-P est positionné. Les champs nécessaires pour le mécanisme de commande de sécurité spécifique indiqué à l'article 10 sont indiqués ci-dessous (voir la Figure 13.11).

Enciphered-Auth-Data	Key Info
(Note 1)	(Note 2)

NOTES

1 La longueur du champ Enciphered-Auth-Data dépend de l'algorithme de codage utilisé et est définie par l'attribut SA Enc_Auth_Len.

2 La longueur des informations de clé dépend de la méthode de répartition des clés utilisée. Elle n'est pas incluse si la clé n'est pas modifiée.

Figure 13-11 – Contenu de la CSC PDU

13.5.7 Enciphered-Auth-Data (données d'authentification codées) (spécifiques des mécanismes)

Voir la Figure 13-12

Ce champ contient un numéro qui est utilisé pour l'authentification et, s'il est sélectionné comme numéro de séquence d'intégrité, sa longueur est définie dans le cadre des attributs SA. Lorsqu'il est envoyé de l'entité appelante à l'entité appelée, l'attribut Your-Initial-ISN est égal à 0.

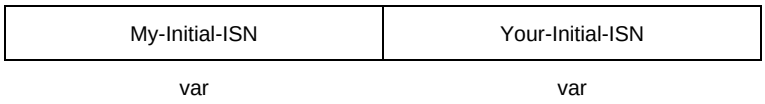


Figure 13-12 – Champ Enciphered-Auth-Data

13.5.8 Informations de clés spécifiques des mécanismes

Selon la méthode de répartition de clés sélectionnée pour l'association de sécurité, ce paramètre n'est pas présent (ce qui indique qu'une clé existante doit être utilisée) ou contient l'un des éléments suivants en fonction du mécanisme de répartition de clés (kdm) attribué à l'association SA:

kdm_mutual –	Clé codée à l'aide de la clé KEK (clé de codage de clés) mutuelle
kdm_asymmetric_single –	Clé codée à l'aide de la clé publique du destinataire
kdm_asymmetric_double –	Clé codée à l'aide de la clé privée de l'expéditeur et de la clé publique du destinataire
kdm_distributed –	Référence de clé
kdm_other –	Contenu défini à titre privé

La présence de ce champ résulte implicitement de la longueur de contenu comparée à l'attribut SA Enc_Auth_Len.

14 Conformité

14.1 Conditions de conformité statique

14.1.1 Classes de conformité

Le système doit permettre la mise en œuvre de l'une ou l'autre, ou des deux, classes de conformité suivantes:

a) mode NLSP-CL;

b) mode NLSP-CO.

La mise en œuvre de ces classes de conformité est définie en termes de capacités indiquées aux 14.1.2 et 14.1.3.

Chacune de ces classes de conformité doit, à titre facultatif, pouvoir être mise en œuvre par l'utilisation des mécanismes de sécurité pris en charge par la présente Recommandation | Norme internationale.

L'utilisation des mécanismes de sécurité pris en charge par la présente Recommandation | Norme internationale est définie en termes de conditions requises pour les mécanismes de sécurité, comme indiqué au 14.1.5.

14.1.2 Capacités offertes dans le mode NLSP-CL

14.1.2.1 Services de sécurité

Un système conforme au mode NLSP-CL doit permettre la mise en œuvre des services suivants:

a) Un ou plusieurs des services suivants:

1) confidentialité des données en mode sans connexion;

2) intégrité en mode sans connexion;

3) authentification de l'origine des données.

b) A titre facultatif, le contrôle d'accès.

c) A titre facultatif, la confidentialité du flux de trafic.

14.1.2.2 Portée de la protection

Un système déclaré conforme au mode NLSP-CL doit permettre la mise en œuvre de l'une ou l'autre, ou des deux, fonctions suivantes:

a) protection de tous les paramètres de service NLSP;

b) protection des données d'utilisateur NLSP.

Un système déclaré conforme au mode NLSP-CL peut, à titre facultatif, permettre la mise en œuvre du service suivant:

c) absence de protection.

14.1.2.3 Autres capacités

Lorsque le mode NLSP-CL est mis en œuvre, le système doit pouvoir émettre et/ou recevoir une SDT PDU.

14.1.3 Capacités offertes dans le mode NLSP-CO

14.1.3.1 Services de sécurité

Un système conforme au mode NLSP-CO doit permettre la mise en œuvre des services de sécurité suivants:

a) Un ou plusieurs des services suivants:

1) confidentialité des données en mode connexion;

2) intégrité en mode connexion sans reprise;

3) authentification de l'entité homologue.

b) A titre facultatif, le contrôle d'accès.

c) A titre facultatif, la confidentialité du flux de trafic.

14.1.3.2 Portée de la protection

Un système déclaré conforme au mode NLSP-CO doit permettre la mise en œuvre de l'un ou de plusieurs des services suivants:

a) protection de tous les paramètres de service NLSP;

b) protection des données d'utilisateur NLSP, y compris les données d'utilisateur NLSP contenues dans les primitives NLSP-CONNECT et NLSP-DISCONNECT;

c) protection des données d'utilisateur NLSP pendant le transfert des données.

Un système déclaré conforme au mode NLSP-CO peut, à titre facultatif, permettre la mise en œuvre du service suivant:

d) absence de protection.

14.1.3.3 Autres capacités

Lorsque le mode NLSP-CO est pris en charge, le système doit pouvoir:

a) initialiser et/ou accepter une connexion;

b) émettre et recevoir une CSC PDU;

c) émettre et/ou recevoir au moins l'un des éléments suivants:

1) données protégées à l'aide des mécanismes d'encapsulation fondés sur l'attribut No_Header, comme indiqué aux 6.4.1.2 et 6.4.2.2;

2) données encapsulées fondées sur la SDT PDU comme indiqué aux 6.4.1.1 et 6.4.2.1;

d) mettre en œuvre au moins l'un des modes d'établissement de connexion NLSP définis au 8.5;

e) à titre facultatif, permettre les échanges de tests;

f) à titre facultatif, permettre la mise en œuvre du protocole SA dans la bande.

14.1.4 Utilisation des PDU

Le Tableau 14-1 indique si l'utilisation d'une PDU donnée est obligatoire ou facultative pour un mode de mise en œuvre donné.

Tableau 14-1 – Mise en œuvre des PDU par le protocole NLSP

PDU	Condition d'utilisation
SDT PDU	Obligatoire pour le mode CL Obligatoire si le mode CO et l'encapsulation fondée sur la SDT PDU sont mis en œuvre
SA PDU	Facultative si le protocole SA-P est mis en œuvre
CSC PDU	Obligatoire pour le mode NLSP-CO

14.1.5 Conditions statiques requises pour les mécanismes

Un système censé permettre la mise en œuvre des mécanismes de sécurité définis dans la présente Recommandation de l'UIT-T | Norme internationale doit répondre aux conditions suivantes en ce qui concerne les mécanismes sélectionnés.

a) Chaque système censé permettre la mise en œuvre des services de sécurité confidentialité en mode connexion ou sans connexion doit assurer ces services par l'utilisation d'un mécanisme de codage.

b) Chaque système censé permettre la mise en œuvre des services de sécurité intégrité en mode sans connexion ou intégrité en mode connexion sans reprise doit assurer ces services à l'aide d'un mécanisme utilisant le champ ICV défini au 13.3.3.2 et, à titre facultatif, le champ ISN défini au 13.3.5.1.

c) Chaque système censé permettre la mise en œuvre du service de sécurité confidentialité du flux de trafic doit assurer ce service à l'aide d'un mécanisme utilisant le champ remplissage de trafic défini au 13.3.5.3.

d) Chaque système censé permettre la mise en œuvre du service de sécurité authentification de l'origine des données doit assurer ce service à l'aide d'un mécanisme de codage ou d'un mécanisme cryptographique utilisant le champ ICV défini au 13.3.3.2.

e) Chaque système censé permettre la mise en œuvre du service de sécurité authentification de l'entité homologue doit utiliser le champ enciphered-auth-data défini au 13.5.7.

14.2 Conditions requises pour la conformité dynamique

14.2.1 Conditions générales

a) Le système doit pouvoir correctement générer, accepter tous les éléments de protocole valides qui prennent en charge chaque classe et mode de fonctionnement auxquels il est déclaré conforme, et répondre à ces mêmes éléments.

b) Le système doit répondre correctement à toutes les séquences incorrectes d'éléments de protocole NLSP.

14.2.2 Conditions spécifiques

Pour chaque classe de conformité à laquelle le système est déclaré apte et pour chaque option des conditions de conformité statique mise en œuvre, le système doit se comporter extérieurement d'une manière compatible avec la mise en œuvre des fonctions suivantes:

a) les fonctions de protocole communes définies à l'article 6;

b) pour le mode NLSP-CL, les fonctions de protocole définies à l'article 7;

c) pour le mode NLSP-CO, les fonctions de protocole définies à l'article 8;

d) pour les systèmes NLSP-CL capables d'utiliser des procédures spécifiques des mécanismes, les fonctions de protocole définies à l'article 11;

e) pour les systèmes NLSP-CO capables d'utiliser des procédures spécifiques des mécanismes, les fonctions de protocole définies à l'article 10 pour la commande de sécurité de connexion et les fonctions de protocole d'encapsulation définies aux articles 11 ou 12;

f) la structure et le codage de PDU comme indiqué à l'article 13, Structure et codage des PDU.

14.3 Déclaration de conformité d'une instance de protocole

Une déclaration de conformité d'une instance de protocole (PICS) présentée dans l'Annexe D doit être remplie pour toute revendication de conformité d'un mode de mise en œuvre avec la présente Recommandation | Norme internationale. La déclaration PICS doit être établie conformément au formulaire PICS approprié.

Annexe A

Mise en correspondance des primitives UN avec la Rec. X.213 du CCITT | ISO 8348

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

Tableau A-1

Primitive UN	Acheminée par la primitive	Observations
UN-UNITDATA	N-UNITDATA	Mise en correspondance simple de la primitive UN avec la primitive N-UNITDATA de la Rec. X.213 du CCITT | ISO 8348/AD1
UN-CONNECT	N-CONNECT	Paramètres mis en correspondance avec les paramètres équivalents de la Rec. X.213 du CCITT | ISO 8348 sauf: – les données d'authentification UN enchaînées avec les données d'utilisateur UN qui sont mises en correspondance avec les données d'utilisateur dans les primitives N-CONNECT
UN-DATA	N-DATA	Mise en correspondance simple. Tous les paramètres sont mis en correspondance avec les paramètres équivalents de la Rec. X.213 du CCITT | ISO 8348
UN-EXPEDITED-DATA	N-EXPEDITED-DATA	Mise en correspondance simple
UN-DATA-ACKNOWLEDGE	N-DATA-ACKNOWLEDGE	Mise en correspondance simple
UN-DISCONNECT	N-DISCONNECT	Mise en correspondance simple

Annexe B

Mise en correspondance des primitives UN avec la Rec. X.25 du CCITT | ISO 8208

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

Dans les environnements OSI, la mise en correspondance entre les primitives de service UN et le protocole de ISO 8208 ou de la Rec. X.25 du CCITT est définie dans ISO 8878 pour les primitives de service de couche réseau équivalentes, à l'exception du paramètre d'authentification UN «UN-CONNECT» qui est acheminé à l'aide du service complémentaire de protection de l'ETTD.

Dans le Tableau B.1, la colonne centrale indique les paquets de ISO 8208 ou de la Rec X.25 utilisés pour acheminer les primitives UN. Dans ce cas, ISO 8208 ou la Rec. X.25 peut faire l'objet de toute application autorisée par la présente Recommandation | Norme internationale et, par exemple, le bit Q peut être invoqué. Ces éléments de service spécifiques de ISO 8208 ou de la Rec. X.25 sont pris en charge sans changement par le protocole NLSP.

Tableau B-1

Primitive UN	Acheminée par les paquets	Observations
UN-UNITDATA	Non applicable	
UN-CONNECT	APPEL	Tous les paramètres sont mis en correspondance avec les services complémentaires en mode paquets d'APPEL équivalents de la Rec. X.25 | ISO 8208, sauf le paramètre d'authentification UN qui est acheminé à l'aide du service complémentaire de protection de l'ETTD
UN-DATA	DONNÉES	Mise en correspondance simple
UN-EXPEDITED-DATA	INTERRUPTION	Mise en correspondance simple
UN-DATA-ACKNOWLEDGE	RR ou RNR	Mise en correspondance simple
UN-DISCONNECT	LIBÉRATION	Mise en correspondance simple

Annexe C

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

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

C.1 Vue d'ensemble

La présente annexe définit un protocole pour l'utilisation d'un mécanisme asymétrique permettant l'établissement et l'abandon/la libération de l'association SA. Il permet aux entités NLSP 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 assure logiquement les fonctions distinctes suivantes:

a) un échange de jetons de clé est utilisé pour établir un secret partagé. La forme de ces jetons est spécifique des mécanismes. Un exemple de jetons de clé spécifiques des mécanismes permettant l'échange de clés exponentielles, également appelé échange de Diffie Hellman, est décrit dans l'Annexe H;

b) des certificats, des signatures numériques et des éléments résultant de l'échange de jetons de clé 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 NLSP doit avoir préétabli les informations suivantes:

a) les mécanismes qu'elle met en œuvre, exprimés par:

   1) une liste des ensembles de règles ASSR mis en application;

   2) l'ensemble des services de sécurité assurés pour chacun des ensembles de règles ASSR indiqués en 1) ci-dessus;

b) pour chaque algorithme asymétrique mis en œuvre, une paire de clés asymétriques qui peut être utilisée par l'entité NLSP pour signer des données à des fins d'authentification;

c) pour chaque algorithme asymétrique mis en œuvre, un certificat émanant de toute autorité de confiance qui identifie l'entité NLSP 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 NLSP avec lesquelles cette entité NLSP 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) création 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 NLSP:

a) identificateurs SA-ID local et distant;

b) services de sécurité à utiliser 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 des mêmes services de sécurité sélectionnés, des mêmes mécanismes avec leurs paramètres et du même ensemble d'étiquettes de sécurité que 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 attribuées.

Dans le cas du protocole NLSP en mode sans connexion, l'identificateur SA-ID doit, après la libération d'une association SA, être bloqué. Lorsqu'il est bloqué, l'identificateur SA-ID ne doit pas être réutilisé. 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 à l'aide de moyens qui sortent du cadre de ce protocole.

Le paramètre entité initiatrice des attributs SA 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 qui répond.

C.2 Echange de jetons de clé (KTE)

Les entités NLSP commencent à mettre en œuvre leur protocole SA en échangeant des jetons de clé 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 du reste des échanges de données de protocole SA.

Le procédé KTE consiste à échanger deux valeurs «Key-Token-1» (jeton de clé nº 1) et «Key-Token-2» (jeton de clé nº 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 H. Les valeurs échangées sont utilisées ensuite par les deux 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 permettant 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 d'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*.

C.3 Authentification de protocole SA

Pour qu'une entité NLSP 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 NLSP échangent des certificats et des signatures numériques (telles que celles qui sont définies dans la Rec. X.509 du CCITT | ISO/CEI 9594-8) pour vérifier mutuellement leur identité. Un certificat contient au minimum certaines informations d'identification d'une NLSPE plus la clé publique de cette entité.

Le certificat est certifié par une autorité de confiance et fourni au protocole NLSP à l'aide d'une procédure qui sort du cadre du protocole NLSP. Le certificat porte la signature d'authentification de l'autorité de confiance. Une entité NLSP 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 Recommandation | Norme internationale. Pour qu'une entité 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 du protocole en cours de mise en œuvre. A cet effet, les deux entités communicantes A (entité initiatrice de l'association SA) et B (entité répondante) procèdent comme suit:

a) le contenu SA est créé, y compris le certificat de l'entité A et le jeton de clé nº 3 (calculé en utilisant un algorithme tel que celui décrit dans l'Annexe H), puis il est signé (utilisant par exemple la signature d'authentification définie dans la Rec. X.509 du CCITT | ISO/CEI 9594-8). Cette signature exclut l'échange ID et la longueur de contenu. Les contenus SA, y compris la signature et la longueur de contenu mais en excluant l'échange ID, 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 nécessaire à l'algorithme utilisé;

b) le contenu SA qui achemine la négociation d'attributs SA (voir C.4) ou les raisons de l'abandon/la libération (voir C.5) est créé puis signé et codé comme pour a) ci-dessus à l'aide d'informations équivalentes relatives à B et au jeton de clé nº 4 au lieu du jeton de clé nº 3.

Chaque entité vérifie la signature d'authentification de l'entité homologue en décodant d'abord les données reçues lors de l'échange puis en vérifiant la signature et en contrôlant le jeton de clé pour se protéger des attaques à répétition. La vérification nécessite l'utilisation de la clé publique de l'entité homologue et du processus agréé pour la vérification de la signature.

C.4 Négociation d'attributs SA

C.4.1 Sélection des services de sécurité

Selon les décisions prises localement, l'entité NLSP initiatrice établit un ensemble d'une ou de 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.

Selon les décisions prises localement, l'entité NLSP 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 aux deux entités NLSP de sélectionner des services de sécurité conformes à la politique de sécurité locale.

C.4.2 Négociation de l'ensemble d'étiquettes

En fonction de sa politique de sécurité locale, l'entité NLSP 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:

a) une référence qui peut, pour des raisons d'efficacité, être transmise ultérieurement au lieu de l'étiquette pendant la durée de la SA; et

b) la sémantique complète de l'étiquette.

En fonction de sa politique de sécurité locale, l'entité NLSP 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 NLSP 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 NLSP de sélectionner un ensemble d'étiquettes conforme à sa politique de sécurité locale.

C.4.3 Sélection de clés et de numéros ISN

Selon les décisions prises localement, l'entité NLSP initiatrice sélectionne les parties de la chaîne binaire qui résulte de l'échange KTE pour les utiliser comme clés et/ou numéros ISN pendant les communications (c'est-à-dire les communications NLSP et non les communications de protocole SA) avec l'entité NLSP 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 EKE. La longueur de la clé/de l'ISN est déterminée à partir des paramètres associés au service sélectionné. Un ensemble de pointeurs est envoyé à l'entité NLSP 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 NLSP destinataire détermine localement les parties de la chaîne binaire résultant de l'échange EKE qu'elle utilisera comme clés/numéros ISN. L'entité NLSP 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 NLSP 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.

NOTES

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

2 Il n'est pas nécessaire d'utiliser cette procédure si les positions pour la sélection des clés et des numéros ISN sont connues *a priori*.

C.4.4 Négociation de divers attributs SA

Selon les décisions prises localement, l'entité NLSP initiatrice détermine la valeur des attributs SA suivants pour l'association SA en cours d'établissement:

a) maintien de ces attributs SA lors de la déconnexion (protocole NLSP-CO seulement);

b) protection des paramètres CO (protocole NLSP-CO seulement);

c) utilisation de l'option No_Header (protocole NLSP-CO seulement).

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

Selon les décisions prises localement, l'entité NLSP 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.

C.4.5 Nouveau codage de clés

Si une association SA est en cours d'établissement pour coder à nouveau une ancienne association SA, seule la sélection des clés et numéros ISN est effectuée. Au lieu de la négociation des services, de l'ensemble d'étiquettes et de 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.

C.5 Abandon/libération de l'association SA

Une entité peut indiquer qu'elle n'utilise plus une association de sécurité par un échange bilatéral de SA PDU avec un code de raison signé et codé à l'aide des procédures définies au C.3.

C.6 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 clés exponentielles (EKE) 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 C.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 C.3.

C.6.1 (Premier) Echange de jetons de clé (KTE)

C.6.1.1 Demande d'initialisation d'un protocole SA

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

L'entité NLSP 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 proposés qui pourrait être utilisée 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'attribut ASSR_ID et les services de sécurité de confidentialité sélectionnés. Il n'est pas nécessaire que cette liste soit envoyée si des mécanismes ont été convenus à l'avance;

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 d'intégrité sélectionnés. Il n'est pas nécessaire que cette liste soit envoyée si des mécanismes ont été convenus par avance.

NOTES

1 Les services de sécurité de confidentialité sélectionnés ne doivent identifier qu'un algorithme de codage symétrique et son mode de fonctionnement. Les services de sécurité d'intégrité sélectionnés ne doivent identifier qu'un algorithme asymétrique et son système de signature numérique associé.

2 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 NLSP initiatrice transmet à nouveau sa PDU du premier échange. Les nouvelles transmissions sont limitées à un nombre fini qui est déterminé localement.

C.6.1.2 Réception de la première SA PDU par l'entité destinataire

A la réception de la première SA PDU, l'entité NLSP destinataire assure les fonctions suivantes et envoie les informations suivantes à l'entité initiatrice:

a) l'attribut My_SA-ID reçu est placé dans le champ Your_SA-ID de l'en-tête générique comme indiqué au 13.4;

b) un identificateur SA-ID disponible est sélectionné et envoyé comme attribut My_SA-ID de l'entité expéditrice;

c) selon les décisions prises localement, l'entité NLSP destinataire renvoie les informations PCI suivantes à l'entité expéditrice:

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) selon les décisions prises localement, l'entité NLSP 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 de 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 NLSP 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.

C.6.2 (Deuxième) Echange de négociation de l'authentification et de la sécurité

C.6.2.1 Réception de la première SA PDU par l'entité initiatrice

A la réception de la première SA PDU, l'entité NLSP initiatrice assure les fonctions suivantes:

a) l'attribut My_SA-ID reçu est placé dans le champ Your_SA-ID de l'en-tête générique comme indiqué au 13.4;

b) le certificat de l'entité initiatrice associé au mécanisme d'intégrité sélectionné est placé dans le champ de contenu certificat;

c) l'entité initiatrice établit le jeton de clé nº 3;

d) une liste des services de sécurité proposés qui pourrait être utilisée pour protéger la communication NLSP est placée dans le champ de contenu «sélection des services»;

e) un ensemble d'étiquettes proposées qui pourrait être protégé à l'aide de cette association SA pendant la communication NLSP est placé dans l'attribut Label_Def;

f) un ensemble de sélections de clés/numéros ISN est placé dans l'attribut «sélection de clés»;

g) les divers attributs SA nécessaires pour cette association SA sont placés dans des marqueurs SA;

h) si l'établissement de l'association SA consiste à coder à nouveau une ancienne SA, l'attribut Old Your_SA-ID est réglé à la valeur de l'identificateur SA-ID de l'ancienne association SA qui fait l'objet d'un nouveau codage. 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 C.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 NLSP 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 renvoyée.

C.6.2.2 Réception de la PDU du deuxième échange par l'entité destinataire

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

a) l'attribut My_SA-ID reçu est placé dans le champ Your_SA-ID de l'en-tête générique comme indiqué au 13.4;

b) les points suivants sont vérifiés. Si la vérification d'un point quelconque échoue, l'association SA est rejetée et un champ d'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 nº 3 est vérifié pour déterminer s'il est valide;

   3) l'ensemble de services de sécurité proposés est vérifié pour déterminer si l'un quelconque d'entre eux 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 d'entre elles 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 décrits en c), d) ci-dessous ne peuvent être envoyés.

Sous réserve que toutes les vérifications aient réussi, 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 les communications NLSP sont envoyés. Si l'ensemble des services proposés contenait un seul élément, aucune information PCI n'est renvoyée;

c) l'entité destinataire établit le jeton de clé nº 4;

d) le sous-ensemble sélectionné d'étiquettes proposées qui pourrait être protégé à l'aide de cette association SA pendant la communication NLSP est envoyé;

e) un ensemble de pointeurs de clé/numéro ISN est envoyé. Si les clés que l'entité initiatrice propose à l'entité destinataire d'utiliser sont acceptables, aucune nouvelle valeur n'est envoyée;

f) protection du contenu SA comme indiqué au C.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.

C.6.3 Echange pour la libération/l'abandon de l'association SA

C.6.3.1 Demande d'initialisation de la libération/de l'abandon de l'association SA

L'entité NLSP 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 nº 3 est établi, autrement le jeton de clé nº 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) protection du contenu SA comme indiqué au C.3.

Dans le cas du mode CO, si une PDU de confirmation résultant de la demande d'abandon/de libération 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 une PDU de confirmation résultant de la demande d'abandon/de libération n'est pas renvoyée après une temporisation, l'entité NLSP 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.

C.6.3.2 Réception d'une demande d'abandon/de libération SA

A la réception de la PDU de confirmation d'abandon/de libération SA, l'entité NLSP 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 nº 3 est établi, autrement le jeton de clé nº 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) protection du contenu SA comme indiqué au C.3.

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

C.7 SA PDU – Contenu SA

Pour ce protocole SA spécifique, le format du champ de contenu SA de la SA PDU défini au 13.4 est indiqué sur la Figure C.1.

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

Figure C.1 – Contenu SA

C.7.1 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.

C.7.2 Longueur de contenu

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

C.7.3 Champs de contenu

Le codage du type de champ de contenu est défini au 13.2. Les champs de contenu SA-P (c'est-à-dire A0-BF) utilisés par les procédures de la présente annexe sont indiqués ci-dessous:

Valeur	*Type de champ de contenu*
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	Label-Def
AA	Marqueurs SA
AB	Sélection de clés
AC	ASSR
AD	Jeton de clé n^{o} 3
AE	Jeton de clé n^{o} 4
AF-BF	Réservé pour utilisation future

NOTE – D'autres codes sont réservés pour utilisation privée au 13.2 du texte principal de la présente Recommandation de l'UIT-T | Norme internationale.

La sélection de services, la raison du rejet SA, l'attribut Label-Def, les marqueurs SA et les champs de sélection de clés sont optionnels dans cette définition spécifique du contenu du protocole SA.

C.7.3.1 My_SA-ID

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

C.7.3.2 Old Your_SA-ID

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

C.7.3.3 Key-Token-1, Key-Token-2, Key-Token-3 et Key-Token-4

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

C.7.3.4 Signature numérique d'authentification – Certificat

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

C.7.3.5 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 protocole 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 NLSP protégées par l'association SA en cours d'établissement.

Ce champ doit suivre une occurrence du paramètre ASSR et peut être inclus une ou plusieurs fois dans la PDU du premier ou du deuxième échange pour former un ensemble de services de sécurité proposé pour la négociation. Chaque paramètre est en relation avec le paramètre ASSR immédiatement précédent.

Ce paramètre contient une séquence d'octets indiquant les niveaux nécessaires 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 0. Un seul octet de valeur 255 indique que les services de sécurité sélectionnés ont été préétablis.

Octet	*Signification*
1	Confidentialité en mode sans connexion/confidentialité en mode connexion
2	Intégrité en mode sans connexion/intégrité en mode connexion sans reprise
3	Authentification de l'origine des données/authentification de l'entité homologue
4	Contrôle d'accès
5	Confidentialité du flux de trafic

C.7.3.6 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:

Valeur	*Signification*
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	Confidentialité du flux de trafic non prise en charge
6	Mécanisme de confidentialité rejeté
7	Mécanisme d'intégrité rejeté
8	Mécanisme de contrôle d'accès rejeté
9	Mécanisme d'authentification rejeté
10	Confidentialité du flux de trafic rejetée
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	Attribut No_Header rejeté

C.7.3.7 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.

C.7.3.8 Label-Def

Ce champ facultatif n'est utilisé que dans la PDU de deuxième échange. Le champ Label-Def peut être inclus une ou plusieurs fois pour:

a) proposer un ensemble d'étiquettes de sécurité s'il est utilisé par l'entité appelante. L'entité initiatrice doit toujours utiliser les deux sous-champs;

b) sélectionner un sous-ensemble de l'ensemble d'étiquettes proposé s'il est utilisé par l'entité destinataire. L'entité destinataire ne doit utiliser que le sous-champ Label_Ref.

Le champ Label-Def est subdivisé en deux sous-champs:

a) un sous-champ Label_Ref à deux octets (la valeur FF FF hex ne doit pas être utilisée car elle est réservée pour une référence d'étiquette NULL);

b) un sous-champ Label dont le contenu est défini au 13.3.4.3.7.

Le champ Label_Ref est un nombre associé à l'étiquette de sécurité définie dans le sous-champ Label. Le champ Label_Ref est utilisé dans d'autres PDU comme variante pour transporter l'étiquette de sécurité associée.

C.7.3.9 Sélection de clés

Ce champ facultatif ne doit être utilisé que dans la PDU du deuxième échange. Il peut apparaître un nombre quelconque de fois dans le contenu SCI.

Ce champ est subdivisé en trois sous-champs:

a) marqueur d'utilisation (deux octets);

b) information de sélection de clés (deux octets);

c) référence de clé (variable).

C.7.3.9.1 Marqueurs d'utilisation

Ce sous-champ contient des marqueurs indiquant les besoins de sécurité pour lesquels la clé définie dans le précédent sous-champ doit être utilisée. Les bits sont codés de telle sorte que la valeur 0 ait la signification FAUX, la valeur 1 ayant la signification VRAI. La clé peut être utilisée pour toute combinaison des besoins indiqués ci-dessous. Les combinaisons admissibles dépendent de la politique de sécurité locale.

Bit n°	*Service*	*Données*	*Origine des données*
Octet 1			
1	Confidentialité	Normales	Initiateur SA
2	Confidentialité	Normales	Répondeur SA
3	Confidentialité	Exprès	Initiateur SA
4	Confidentialité	Exprès	Répondeur SA
5	Génération ICV	Normales	Initiateur SA
6	Génération ICV	Normales	Répondeur SA
7	Génération ICV	Exprès	Initiateur SA
8	Génération ICV	Exprès	Répondeur SA
Octet 2			
1	Authentification		Initiateur SA
2	Authentification		Répondeur SA
3	ISN	Normales	Initiateur SA
4	ISN	Normales	Répondeur SA
5	ISN	Exprès	Initiateur SA
6	ISN	Exprès	Répondeur SA

L'entité qui répond peut neutraliser les sélections pour son propre usage.

C.7.3.9.2 Informations de sélection de clé

Ce champ indique la position, dans la chaîne binaire résultant de l'échange EKE, où une clé sélectionnée doit prendre sa valeur. La longueur de la clé est déterminée à partir des services de sécurité associés sélectionnés qui identifient 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.

C.7.3.9.3 Référence de clé

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

C.7.3.10 Marqueurs SA

Ce champ facultatif ne doit être utilisé que dans la PDU du deuxième échange. 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.

Bit	*Attribut SA*
1	Retain_on_Disconnect
2	Param_Prot
3	No_Header
4-8	Réservé pour utilisation future

Les bits 4 à 8 sont réglés à 0 lors de la transmission et sont ignorés lors de la réception.

C.7.3.11 ASSR

Ce champ doit être présent si le champ sélection de service est présent. C'est l'identificateur d'objet (défini dans ISO/CEI 9834-3) qui identifie l'ensemble de règles de sécurité définissant les mécanismes à appliquer en fonction de la qualité de service sélectionnée en matière de protection.

Ce champ peut être présent plusieurs fois, auquel cas les paramètres de sélection de service qui suivent chaque occurrence sont en relation avec le paramètre ASSR immédiatement précédent.

Annexe D

Formulaire PICS NLSP [2)]

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

D.1 Introduction

The supplier of a protocol implementation which is claimed to conform to this ITU-T Recommendation | International Standard shall complete the following Protocol Implementation Conformance Statement (PICS) proforma.

A completed PICS proforma is the PICS for the implementation in question. The PICS is a statement of which capabilities and options of the protocol have been implemented. The PICS can have a number of uses, including use:

- by the protocol implementor, as a check-list to reduce the risk of failure to conform to the standard through oversight;
- by the supplier and acquirer – or potential acquirer – of the implementation, stated relative to the common basis for understanding provided by the standard PICS proforma;

---

2) 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.

- by the user – or potential user – of the implementation, as a basis for initially checking the possibility of interworking with another implementation (note that, while interworking can never be guaranteed, failure to interwork can often be predicted from incompatible PICSs);

- by a protocol tester, as the basis for selecting appropriate tests against which to assess the claim for conformance of the implementation.

D.2 Abbreviations and Special Symbols

D.2.1 Status Symbols

M Mandatory

O Optional

O.<n> Optional, but support of at least one of the group of options labelled by the same numeral <n> is required

X Prohibited

<item> Conditional-item symbol, dependent upon the support marked for <item> (see D.3.4)

D.2.2 General Abbreviations

N/A Not applicable

PICS Protocol Implementation Conformance Statement

D.3 Instructions for Completing the PICS Proforma

D.3.1 General Structure of the PICS Proforma

The first part of the PICS proforma – 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 three major subclauses covering features common to NLSP-CL and NLSP-CO, followed by clauses specific to each of these two modes of operation; these are divided into further 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: all relevant choices are to be marked.

Each item is identified by an item reference in the first column; the second column contains the question to be answered; the third column contains the reference or references to the material that specifies the item in the main body of this ITU-T Recommendation | International Standard. The remaining columns record the status of the item – whether support is mandatory, optional, prohibited or conditional – and provide the space for the answers: see also D.3.4 below.

A supplier may also provide, or can be required to provide, further information, categorised as either Additional Information or Exception Information. When present, each kind of further information is to be provided in a further subclause of items labelled A<i> or X<i> respectively for cross-referencing purposes, where i is any unambiguous identification for the item (e.g. simply a numeral): there are no other restrictions on its format and presentation.

A completed PICS proforma, including any Additional Information and Exception Information, is the Protocol Implementation Conformance Statement for the implementation in question.

NOTE – Where an implementation is capable of being configured in more than one way according, for example, to the items in D.5.1, a single PICS may be able to describe all such configurations. However, the supplier has the choice of providing more than one PICS, each covering some subset of the implementation's configuration capabilities, in case that makes for easier and clearer presentation of the information.

D.3.2 Additional Information

Items of Additional Information allow a supplier to provide further information intended to assist the interpretation of the PICS. It is not intended or expected that a large quantity will be supplied, and a PICS can be considered complete without any such information. Examples might be an outline of the ways in which a (single) implementation can be set up to operate in a variety of environments and configurations; or a brief rationale – based perhaps upon specific application needs – for the exclusion of features which, although optional, are nonetheless commonly present in implementations of the network layer security protocol.

References to items of Additional Information may be entered next to any answer in the questionnaire, and may be included in items of Exception Information.

D.3.3 Exception Information

It may occasionally happen that a supplier will wish to answer an item with mandatory or prohibited status (after any conditions have been applied) in a way that conflicts with the indicated requirement. No pre-printed answer will be found in the Support column for this: instead, the supplier shall write the missing answer into the Support column, together with an X<i> reference to an item of Exception Information, and shall provide the appropriate rationale in the Exception item itself.

An implementation for which an Exception item is required in this way does not conform to ITU-T Recommendation | International Standard.

NOTE – A possible reason for the situation described above is that a defect in this ITU-T Recommendation | International Standard has been reported, a correction for which is expected to change the requirement not met by the implementation.

D.3.4 Conditional Status

The PICS proforma contains a number of conditional items. These are items for which both the applicability of the item itself, and its status if it does apply – mandatory, optional or prohibited – are dependent upon whether or not certain other items are supported.

Individual conditional items are indicated by a conditional symbol of the form <item>:<s> in the status column, where <item> is an item reference that appears in the first column of the table for some other item, and <s> is one of the status symbols M, O, O.n or X.

If the item referred to by the conditional symbol is supported, the conditional item is applicable, its status is given by <s> and the support column is to be completed in the usual way. Otherwise, the conditional item is not relevant and the Not applicable (N/A) answer is to be marked.

Each item whose reference is used in a conditional symbol is indicated by an asterisk in the Item column.

D.4 Identification

D.4.1 Implementation Identification

Supplier	
Contact point for queries about the PICS	
Implementation Name(s) and Version(s)	
Other information necessary for full identification – e.g. name(s) and version(s) of machines and or operating systems; system names	

NOTES

1 Only the first three items are required for all implementations; other information may be completed as appropriate in meeting the requirement for full identification.

2 The terms Name and Version should be interpreted appropriately to correspond with the supplier's terminology (e.g. Type, Series, Model).

D.4.2 Protocol Summary

Identification of protocol specification	CCITT Recommendation X.273 (1994) | ISO/IEC 11577:1994
Identification of amendments and corrigenda to this PICS proforma which have been completed as part of this PICS	CCITT Recommendation X.273 (1994) | ISO/IEC 11577:1994 Am. : Corr. : Am. : Corr. : Am. : Corr. : Am. : Corr. :

Have any exception items been required (see D.3.3)? NOTE – The answer **Yes** means that the implementation does not conform to this ITU-T Recommendation | International Standard.	Yes ☐ No ☐

Date of statement	

D.5 Features Common to NLSP-CO and NLSP-CL

D.5.1 Major Capabilities (Common)

Item	Questions/Features	Reference (subclause)	Status	Support
CO*	Is the connection-mode supported?	5.1	O.1	Yes ☐ No ☐
CL*	Is the connectionless-mode supported?	5.1	O.1	Yes ☐ No ☐
AC	Is Access Control supported?	5.2	O	Yes ☐ No ☐
TFC*	Is Traffic Flow Confidentiality supported?	5.2	O	Yes ☐ No ☐
ParamProt*	Is protection of all NLSP service parameters supported?	5.5.1a	O.2	Yes ☐ No ☐
UserDatProt	Is protection of NLSP Userdata supported?	5.5.1b	O.2	Yes ☐ No ☐
NoProt*	Is no protection supported?	5.5.1c	O	Yes ☐ No ☐
SdtBase*	Is any SDT PDU based encapsulation function supported?	5.5.3	CO:O.3 CL:M ParamProt:M	Yes ☐ No ☐
NoHead	Is any No Header encapsulation function supported?	5.5.3	CO:O.3 CL:X ParamProt:X	Yes ☐ No ☐ N/A ☐
SA-P*	Is any in-band SA-P supported?	5.4.1	O	Yes ☐ No ☐
LabMech*	Is the label mechanism supported?	6.2g, 6.4.1.1e, 6.4.2.1f	SdtBase:O	Yes ☐ No ☐ N/A ☐
SDTMech*	Is the standardised SDT PDU based encapsulation function supported?	11	SdtBase:O	Yes ☐ No ☐ N/A ☐
NoHeadMech	Is the standardised No Header encapsulation function supported?	12	NoHead:O	Yes ☐ No ☐ N/A ☐

D.5.2 PDUs (Common)

Item	Questions/Features	Reference (subclause)	Status	Support on Transmission	Support on Receipt
SDT*	Is the Secure Data Transfer PDU supported on transmision/receive?	6.4.1.1 13.3	SdtBase:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
SA*	Is the Security Association PDU supported on transmission/receive?	5.4.1, 13.4	SA-P:O	Yes ☐ N/A ☐	Yes ☐ N/A ☐

D.5.3 SDT PDU Fields Common to CO and CL and Generic to Mechanisms

Item	Questions/Features	Reference (subclause)	Status	Support on Transmission	Support on Receipt
SdtPID	PID field value 10001011 in each SDT PDU	13.3.2.1	SDT:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
SdtLI	Length Indicator field in each SDT PDU	13.3.2.2	SDT:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
SdtPDUType	PDU Type field with value 01001000 in each SDT PDU	13.3.2.3	SDT:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
SdtContLen	Content Length in each SDT PDU	13.3.4.1	SDT:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
DataType	Data Type field in each SDT PDU	13.3.4.2	SDT:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
UserData	Content field type CO – Userdata	13.3.4.3	SDT:O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
CSAddr	Content field type C2 – Calling/Source NLSP address	13.3.4.3	ParamProt:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
CDAddr	Content field type C3 – Calling/Destination NLSP address	13.3.4.3	ParamProt:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
Label	Content field type C6 – Label	13.3.4.3	LabMech:O.4	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
LabRef	Content field type C7 – Label Reference	13.3.4.3	LabMech:O.4	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
LabelExc	Is the mutual exclusion of label and label reference in any SDT PDU enforced?	13.3.4.3	LabMech:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐

D.5.4 SDT PDU Fields Common to CO and CL with Specific SDT Based Encapsulation Mechanisms

Item	Questions/Features	Reference (subclause)	Status (Note)	Support on Transmission	Support on Receipt
Synch	Crypto synchronisation	11.3, 13.3.3.1	O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
ICV	ICV field	11.3, 13.3.3.2	COInteg:M CLInteg:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
EncPad	Padding for Encipherment	11.3, 13.3.3.3	COConf:O CLConf:O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
SeqNo	Sequence Number Content field	11.3, 13.3.5.1	COInteg:O CLInteg:O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
SinglePad	Single octet general padding field	11.3, 13.3.5.2	O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
TFCPad	Traffic padding	11.3, 13.3.5.3	TFC:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
IntegPad	Padding for Integrity	11.3, 13.3.5.4	COInteg:O CLInteg:O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
NOTE – All the above fields are conditional on SDTMech selected.					

D.5.5 SA PDU Fields Generic to SA-P

Item	Questions/Features	Reference (subclause)	Status	Support on Transmission	Support on Receipt
SaPID	PID field value 10001011 in each SA PDU	13.4.1	SA:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
SaLI	Is the Length Indicator field transmitted in each SA PDU?	13.4.2	SA:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
SaPDUType	PDU Type field with value 01001001 in each SA PDU	13.4.3	SA:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
SaSA-ID	SA-ID field	13.4.4	SA:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
SA-PType	SA-P Type field	13.4.5	SA:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
SAKTE*	Is the example SA protocol using Key Token Exchange supported?	Annex C	SA:O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐

D.5.6 SA PDU Content Fields Specific to Key Token Exchange SA-P

Item	Questions/Features	Reference (subclause)	Status	Support on Transmission	Support on Receipt
SAExchId	Exchange ID	C.7.1	SAKTE:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
ContLen	Is the Length Indicator field transmitted in each SA PDU?	C.7.2	SAKTE:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
MySA-ID	My SA-ID Content field	C.7.3.1	SAKTE:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
OldYrSA-ID	Old Your SA-ID Content field	C.7.3.2	SAKTE:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
KeyTokens	Key-Token-1, Key-Token-2, Key-Token-3 and Key-Token-4 Content fields	C.7.3.3	SAKTE:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
AuthFields	Authentication digital signature and Authentication certificate Content fields	C.7.3.4	SAKTE:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
ServSel*	Service Selection Content field	C.7.3.5	SAKTE:O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
SARejReas	SA Rejection Reason Content field	C.7.3.6	SAKTE:O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
SAAbReas	SA Abort/Release Reason Content field	C.7.3.7	SAKTE:M	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
LabDef	Label Definition Content field	C.7.3.8	SAKTE:O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
KeySel*	Key Selection Content field	C.7.3.9	SAKTE:O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
KeyUse	Usage Flags sub-field	C.7.3.9.1	KeySel:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
KeySelInfo	Key Selection Information sub-field	C.7.3.9.2	KeySel:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
KeyRefx	Key Reference sub-field	C.7.3.9.3	KeySel:O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
SAFlags	SA Flags Content field	C.7.3.10	SAKTE:O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
ASSR	ASSR Content field	C.7.3.11	ServSel:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐

D.5.7 Algorithms Supported

Item	Questions/Features	Reference (subclause)	Status	Support
RegKTE	List of registered Key Token Exchange algorithms supported	–	O	Names: Object Identifers:
UnRegKTE	List the unregistered Exponential Key Exchange algorithms supported	–	O	Names:
RegICV	List the registered names of ICV algorithms supported	–	O	Names: Object Identifers:
UnRegICV	List the unregistered ICV algorithms supported	–	O	Names:
RegConf	List the registered names of Confidentiality algorithms supported	–	O	Names: Object Identifers:
UnRegConf	List the unregistered Confidentiality algorithms supported	–	O	Names:

D.6 Features Specific to NLSP-CL

D.6.1 Major Capabilities (NLSP-CL)

Item	Questions/Features	Reference (subclause)	Status	Support
CLConf*	Is connectionless confidentiality supported?	5.2	CL:O.5	Yes ☐ No ☐ N/A ☐
CLInteg*	Is connectionless integrity supported?	5.2	CL:O.5	Yes ☐ No ☐ N/A ☐
DOA	Is Data Origin Authentication supported?	5.2	CL:O.5	Yes ☐ No ☐ N/A ☐

D.6.2 Initiator/Responder (Connectionless Mode)

Item	Questions/Features	Reference (subclause)	Status	Support
CLXmtProt	Is the implementation capable of transmitting protected connectionless data units?	7.6	CL:O.6	Yes ☐ No ☐ N/A ☐
CLRcvProt	Is the implementation capable of accepting incoming protected connectionless data units?	7.7	CL:O.6	Yes ☐ No ☐ N/A ☐
CLXmt	Is the implementation capable of transmitting unprotected connectionless data units?	7.6.1	NoProt:M	Yes ☐ N/A ☐
CLRcv	Is the implementation capable of accepting incoming unprotected connectionless data units?	7.7.1	NoProt:M	Yes ☐ N/A ☐

D.6.3 Environment (Connectionless Mode)

Item	Questions/Features	Reference (subclause)	Status	Support
CL1	Are the mandatory elements of IS 8348 AD1 supported?	5.2	CL:M	Yes ☐ N/A ☐

D.6.4 SDT PDU Fields (Connectionless Mode)

Item	Questions/Features	Reference (subclause)	Status	Support
SdtSA-ID	SA-ID field transmitted in each SDT PDU?	13.3.2.4	CL:M	Yes ☐ N/A ☐

D.7 Features Specific to NLSP-CO

D.7.1 Major Capabilities (NLSP-CO)

Item	Questions/Features	Reference (subclause)	Status	Support
SNAcP	Is the protocol mapping directly onto CCITT Rec. X.25 | ISO 8208?	5.3, Annex B	CO:O.7	Yes ☐ No ☐
SNISP*	Is the protocol mapping onto CCITT Rec. X.213 | ISO 8348?	5.3, Annex A	CO:O.7	Yes ☐ No ☐
COConf*	Is connection confidentiality supported?	5.2	CO:O.8	Yes ☐ No ☐ N/A ☐
COInteg*	Is connection integrity without recovery supported?	5.2	CO:O.8	Yes ☐ No ☐ N/A ☐
PEA	Is peer entity authentication supported?	5.2	CO:O.8	Yes ☐ No ☐ N/A ☐
ExCSC*	Is Example CSC PDU procedures defined in NLSP supported?	10	CO:O	Yes ☐ No ☐ N/A ☐

D.7.2 PDUs (Connection Mode)

Item	Questions/Features	Reference (subclause)	Status	Support on Transmission	Support on Receipt
CSC*	Connection Security Control PDU	8.5, 13.5	CO:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐

D.7.3 Modes of Connection Establishment/Release

Item	Questions/Features	Reference (subclause)	Status	Support as Calling entity	Support as Called entity
UNConn	NLSP-CONNECT in UN-CONNECT	8.5.1.2	CO:O.9	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
UNConnSAP	NLSP-CONNECT in UN-CONNECT with SA-P	8.5.1.2	CO:O.9	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
UNData	NLSP-CONNECT in UN-DATA	8.5.1.2	CO:O.9	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
UNDataSAP	NLSP-CONNECT in UN-DATA with SA-P	8.5.1.2	CO:O.9	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
DUNDisc	NLSP-DISCONNECT in UN-DISCONNECT	8.10	CO:O.10	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
DUNData	NLSP-DISCONNECT in UN-DATA	8.10	CO:O.10	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐

D.7.4 Environment (Connection Mode)

Item	Questions/Features	Reference (subclause)	Status	Support
CO1	Are the mandatory elements of IS 8348 supported?	5.3	SNISP:M	Yes ☐ N/A ☐
ConOpt1	Does the implementation provide Expedited Data?	8.7	CO:O	Yes ☐ No ☐ N/A ☐
ConOpt3	Does the implementation provide Receipt Confirmation?	8.9	CO:O	Yes ☐ No ☐ N/A ☐

D.7.5 Timers and Parameters (Connection Mode)

Item	Questions/Features	Reference (subclause)	Status	Support
T1	Is the timer between transmitting NLSP-DISCONNECT and issuing UN-DISCONNECT supported?	8.10	CO:O	Yes ☐ No ☐ N/A ☐

D.7.6 SDT PDU Fields (Connection Mode)

Item	Questions/Features	Reference (subclause)	Status (Note)	Support on Transmission	Support on Recceipt
TestData	Content field type C1 – Testdata	13.3.4.3	O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
RAddr	Content field type C4 – Responding NLSP address	13.3.4.3	ParamProt:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
ConfReq	Content field type C8 – Confirmation Request	13.3.4.3	ParamProt:O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
Reason	Content field type C9 – Disconnect Reason	13.3.4.3	ParamProt:O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
NOTE – All the items in D.7.6 are conditional on SDT being supported.					

D.7.7 CSC PDU Fields – Generic (Connection Mode)

Item	Questions/Features	Reference (subclause)	Status	Support on Transmission	Support on Receipt
CscPID	PID field value 10001011 in each CSC PDU	13.5.1	CSC:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
CscLI	Length Indicator field in each CSC PDU	13.5.2	CSC:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
CscPTyp	PDU Type field with a value of xx111111 in each CSC PDU	13.5.3	CSC:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
UNC-UNDFlg	Is the UNC-UND flag in PDU Type field transmitted in each CSC PDU?	13.5.3	CSC:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
SA-PFlg	Is the SA-P flag in PDU Type field transmitted in each CSC PDU?	13.5.3c	CSC:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
CscSA-ID	SA-ID field	13.5.4	CSC:O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
ContLen	Content Length field in each CSC PDU	13.5.5	CSC:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐

D.7.8 Example CSC PDU Content (Connection Mode)

Item	Questions/Features	Reference (subclause)	Status	Support
CscInit	Is the implementation capable of initiating a CSC PDU exchange?	10.3	ExCSC:O.11	Yes ☐ No ☐ N/A ☐
CscResp	Is the implementation capable of responding to a peer initiated CSC PDU exchange?	10.3	ExCSC:O.11	Yes ☐ No ☐ N/A ☐
EncAuth	Enciphered AUTH-DATA field	13.5.7	ExCSC:M	Yes ☐ N/A ☐
KeyInfox	Key Information field	13.5.8	ExCSC:O	Yes ☐ No ☐ N/A ☐

Annexe E

Exposé de certains principes de base du NLSP

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

E.1 Base de protection

La base de la protection des données d'utilisateur dans le protocole NLSP est la PDU de transfert de données sûres (SDT PDU) ou la protection en mode No_Header. La SDT PDU protège les données par une fonction d'encapsulation qui ajoute une valeur de contrôle d'intégrité (ICV) puis la code à des fins de confidentialité. Des champs de remplissage peuvent être placés avec les données protégées pour assurer la confidentialité du flux de trafic et mettre en œuvre des mécanismes ICV par bloc. Un champ de remplissage distinct peut être placé après la valeur ICV pour les mécanismes de codage par bloc.

Avant d'être protégées dans une unité SDT PDU, des informations de commande de sécurité additionnelles (par exemple, étiquette, numéro de séquence) peuvent être placées avec les données d'utilisateur pour créer le champ Octet-String-Before-Encapsulation. Ce champ est ensuite protégé à l'aide d'une fonction d'encapsulation comme indiqué ci-dessus. Un en-tête en clair est placé à l'avant de la PDU pour identifier le type de PDU et l'ensemble des «attributs de sécurité» (clés, etc. – voir l'article 5) utilisés pour protéger l'unité de données. La construction d'une SDT PDU est illustrée sur la Figure E.1 ci-dessous.

Le protocole NLSP-CO utilise une seconde méthode facultative pour protéger les données d'utilisateur NLSP, à savoir la méthode appelée No_Header. Avec cette méthode, les données NLSP sont codées directement sans adjonction d'informations de commande de sécurité ou d'en-tête en clair.

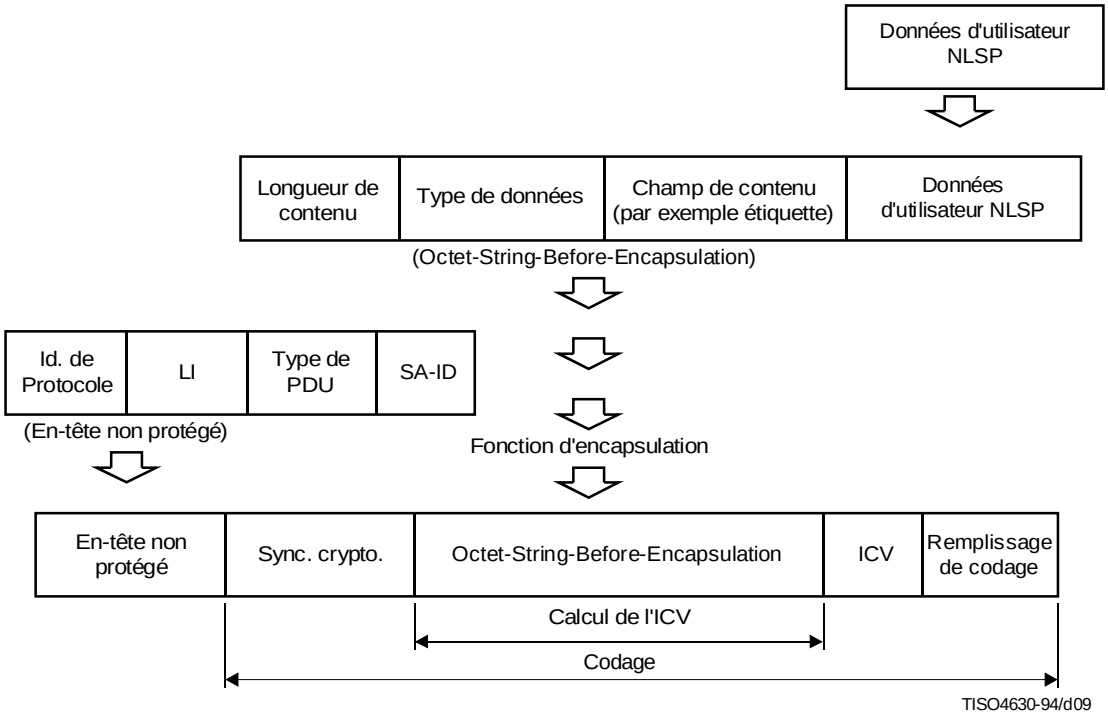


Figure E.1 – Construction d'une PDU de transfert de données sûres

E.2 Service de base et service NLSP

Le protocole NLSP a deux interfaces de service notionnelles. L'une, appelée service NLSP, est l'interface établie avec les protocoles situés «au-dessus du NLSP» (c'est-à-dire les protocoles qui utilisent les communications protégées). L'autre, appelée service UN (réseau de base), est utilisée par le protocole NLSP pour invoquer les protocoles de communication sous-jacents. Le protocole NLSP peut être ajouté en transparence sans influer sur le fonctionnement des protocoles au-dessus et au-dessous du NLSP. L'interface NLSP reflète le service attendu par les protocoles situés au-dessus et le service UN est mis en correspondance avec la forme de service assurée par les protocoles sous-jacents.

Les données d'utilisateur à l'interface de service NLSP sont protégées (par exemple, par encapsulation dans une SDT PDU) avant d'être transmises à l'interface sous-jacente du réseau de base.

Les interfaces de service NLSP et UN sont similaires à celles du réseau OSI sauf en ce qui concerne un aspect important. L'entité desservie par le protocole NLSP n'est pas toujours l'entité de transport et le service UN n'est jamais relié directement à une entité de transport. Comme indiqué plus loin, dans certains cas (voir la Figure E.2), le service NLSP peut être relié à une fonction de relais et de routage dans un système intermédiaire ou même à une entité qui met en œuvre un protocole de couche réseau (voir Figures). Avec le service UN, du point de vue des protocoles sous-jacents, l'interface de service peut se comporter comme une interface de service de réseau OSI mais, du point de vue de l'ensemble de l'empilement OSI, elle est reliée à une entité NLSP dans la couche réseau et elle n'est donc pas une véritable interface de service de réseau OSI.

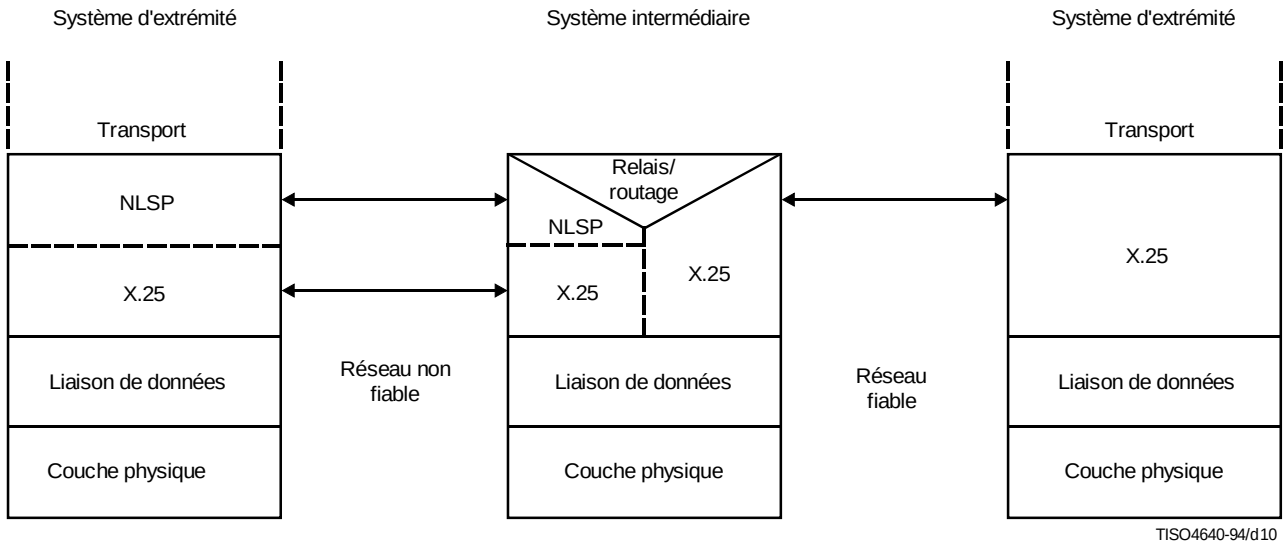
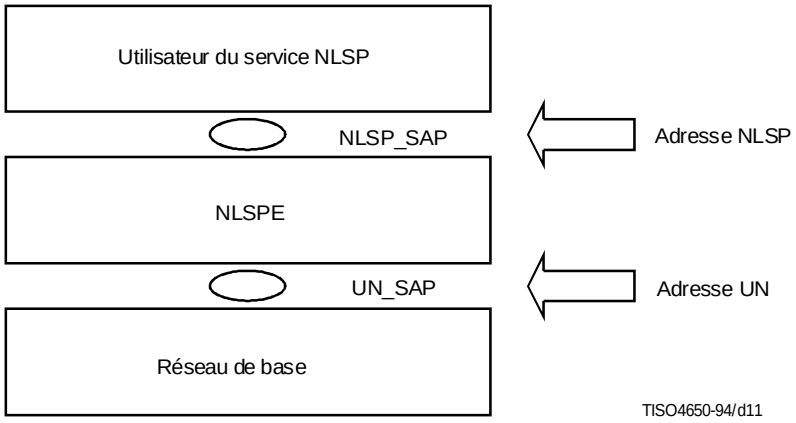


Figure E.2 – Illustration du protocole NLSP-CO avec un système intermédiaire

E.3 Adressage NLSP

L'entité NLSP (NLSPE) est intégrée entre l'utilisateur du service NLSP et le réseau de base. Les points d'accès au service correspondants sont les points NLSP_SAP et UN_SAP. Dans les configurations actuellement mises en œuvre par le protocole NLSP (voir la Figure E.3-1 et la Note ci-dessous), l'adresse qui identifie l'entité rattachée au point NLSP_SAP, par exemple l'utilisateur du service NLSP, est l'adresse NLSP. L'adresse qui identifie l'entité rattachée au point UN_SAP, par exemple la NLSPE, est l'adresse UN. Les NLSPE homologues forment une sous-couche dans la couche réseau. Les limites supérieure et inférieure sont les points d'interaction où les adresses sont échangées. La figure ci-après décrit les points d'accès au service et les adresses correspondantes.



NOTE – Dans les configurations de service de réseau relais en mode CO, l'adresse NLSP peut identifier une adresse NSAP dans un système d'extrémité au lieu d'un point NLSP_SAP dans un système intermédiaire (voir également E.4 et E.5).

Figure E.3-1 – Points SAP supérieur et inférieur, et adresses

Le protocole NLSP est positionné dans la couche réseau. Il peut être placé à la limite inférieure, à la limite supérieure ou entre les deux. Le protocole NLSP et sa limite inférieure de service UN assurent des fonctions différentes selon ce positionnement. De même, les adresses utilisées ont une sémantique différente selon ce positionnement. La Figure E.3-2 indique les emplacements possibles de la NLSPE dans la couche réseau.

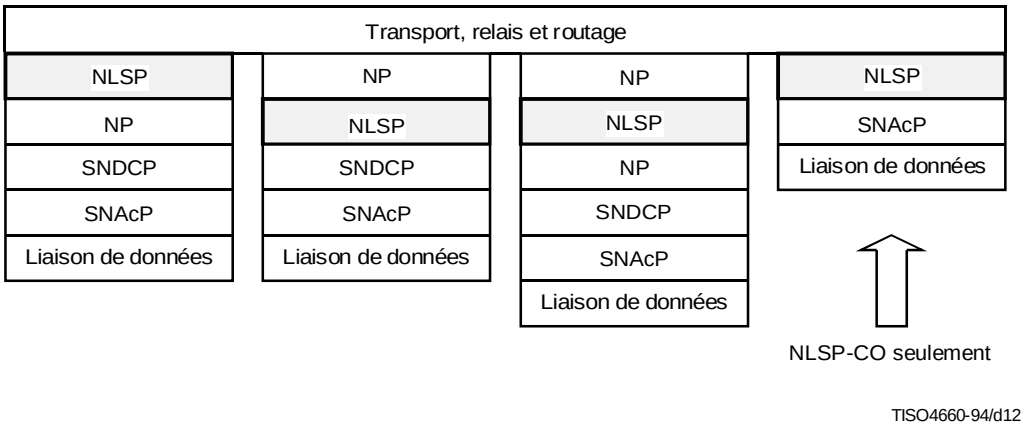


Figure E.3-2 – Positionnement du protocole NLSP dans la couche réseau

Les Figures E.3-3 et E.3-4 indiquent la forme des adresses utilisées dans la couche réseau contenant une sous-couche NLSP à différents emplacements.

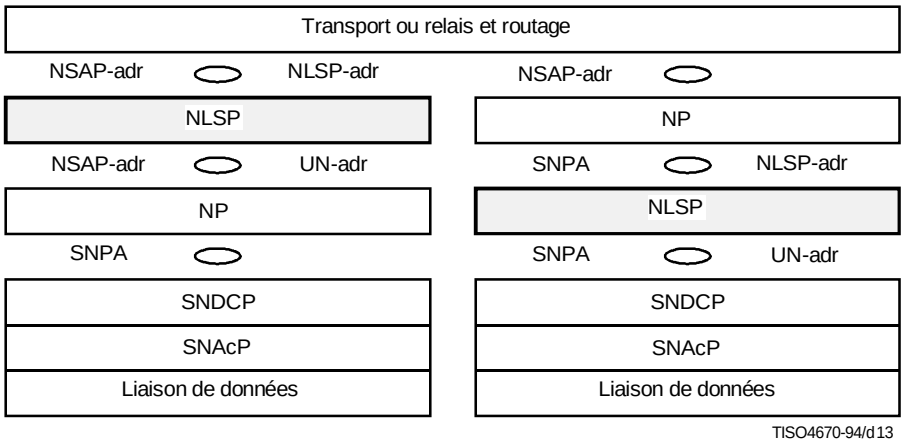


Figure E.3-3 – Adresses dans une couche réseau contenant une sous-couche NLSP – Avec un protocole de réseau (NP) au-dessus/au-dessous du NLSP

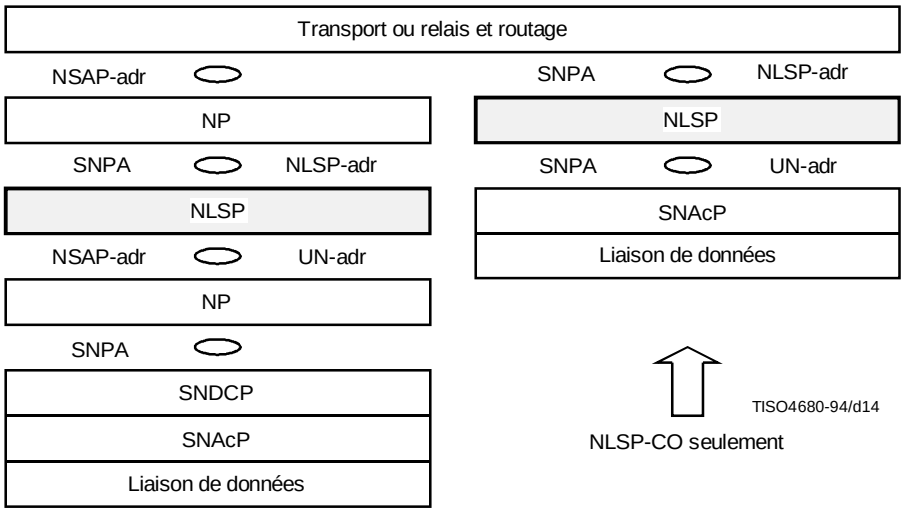


Figure E.3-4 – Adresses dans une couche réseau contenant une sous-couche NLSP – Avec protocole de réseau (NP) au-dessus/au-dessous du NLSP – Sans protocole de réseau

L'adresse NSAP-adr (UN-adr) est utilisée par le protocole NLSP pour l'adressage dans un réseau de base lorsqu'un protocole de réseau (en mode connexion ou sans connexion) est situé sous la sous-couche NLSP. Les adresses NSAP forment un domaine d'adressage encapsulé délimité par la sous-couche NLSP. Les adresses NSAP ont une syntaxe identique en tant qu'adresses NSAP et sont enregistrées à l'aide de la procédure d'enregistrement d'adresse NSAP. Les adresses NSAP formant un domaine de réseau fiable ne sont utilisées que dans un domaine protégé par les sous-couches NLSP.

L'adresse SNPA (adresse de protocole de sous-réseau) peut être identique à l'adresse SNPA déterminée par l'entité NP située au niveau supérieur. Cependant, l'adresse SNPA peut être différente selon l'emplacement de la NLSPE homologue.

Le domaine d'adressage encapsulé peut être considéré comme un sous-réseau virtuel dans un environnement OSI (environnement d'interconnexion de systèmes ouverts) (OSIE). Il est délimité par un groupe d'entités NLSP dans un système ES ou un système IS ayant chacun un empilement de couche réseau identique au-dessus des protocoles de sous-réseau dépendants de la technologie (SNAcP) protocole de convergence dépendant du sous-réseau/réseau (*subnetwork network dependent convergence protocol*). Ces NLSPE ont donc toutes le même emplacement dans la couche réseau.

La Figure E.3-5 indique un scénario possible d'environnement OSIE contenant un réseau UN virtuel délimité par des entités NLSP dans des systèmes ES et IS.

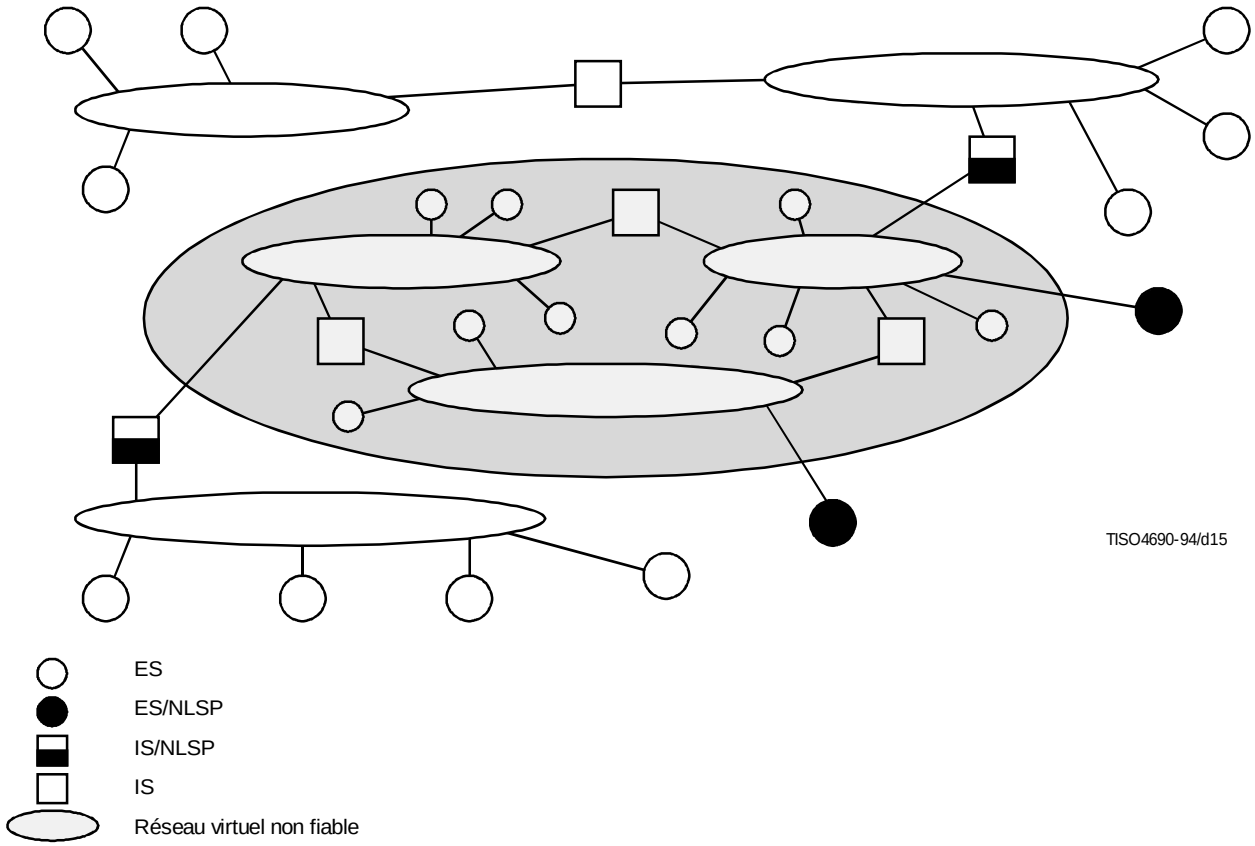


Figure E.3-5 – Réseau UN virtuel dans un environnement OSI

Les empilements de protocoles de couche réseau et l'emplacement des entités NLSP dépendent des protocoles utilisés dans les sous-réseaux et de leur configuration. La sélection est effectuée par une «autorité» qui définit une configuration statique d'une combinaison de réseaux fiables et non fiables, ce qui nécessite des fonctions additionnelles sûres de gestion et de routage qui sortent du cadre de la présente Recommandation de l'UIT-T | Norme internationale.

Selon l'emplacement de la NLSPE dans la couche réseau, l'adresse NLSP et l'adresse UN ont une sémantique différente. En principe, on distingue deux emplacements (voir la Figure E.3-6).

– *Emplacement A* – Le point NLSP_SAP correspond au point OSI NSAP. L'utilisateur du service NLSP est une entité de transport. L'adresse qui identifie l'entité de transport est définie en tant qu'adresse NSAP et est identique à l'adresse NLSP.

  Le réseau de base est considéré comme un domaine de réseau non protégé qui est, en fait, le réseau OSI. L'adresse qui identifie la NLSPE correspond donc à l'adresse OSI NSAP. Cependant, les paramètres transférés dans des primitives de service passant par les limites de points NLSP_SAP et UN_SAP peuvent être différents si les paramètres de service NLSP sont protégés (l'attribut Param_Prot est VRAI).

– *Emplacement B* – La NLSPE est placée entre deux sous-couches réseau. La sous-couche située au-dessus délimite un domaine de réseau protégé, alors que le sous-réseau de base représente un domaine de réseau non protégé.

Dans un système d'extrémité, l'adresse NSAP identifie différents utilisateurs de service de réseau situés au même emplacement dans le système d'extrémité. L'adresse NLSP identifie l'entité de routage du système d'extrémité responsable des fonctions de routage ES.

Dans un système intermédiaire, l'adresse NSAP contient des informations de routage pour la retransmission de NPDU dans le domaine de réseau protégé. L'adresse NLSP identifie l'entité de routage ES/IS dans le système IS. L'adresse UN identifie la NLSPE rattachée au réseau UN.

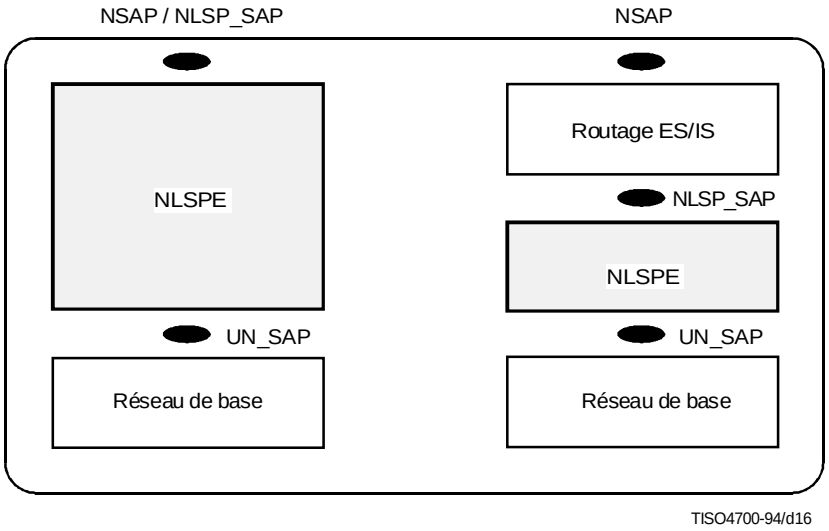


Figure E.3-6 – Emplacements de la NLSPE dans la couche réseau

L'adresse/les adresses NLSP desservies par une NLSPE distante sont contenues dans un attribut SA Adr_Served. L'adresse UN d'une NLSPE distante est contenue dans un attribut SA Peer_Adr:

– si l'attribut Param_Prot est FAUX

Les fonctions NLSP sont limitées à la mise en correspondance des primitives de service du point NLSP_SAP avec le point UN_SAP. L'adresse NSAP est mise directement en correspondance avec l'adresse UN. L'attribut NLSP SA Adr_Served garde la même valeur que l'attribut SA Peer_Adr.

– si l'attribut Param_Prot est VRAI

Le mode est protégé. Les mises en correspondance d'adresses dépendent de l'emplacement de la NLSPE et sont effectuées à l'aide d'attributs Adr_Served et Peer_Adr.

Le Tableau E.1 indique les fonctions de mise en correspondance d'adresse des NLSPE selon leurs divers emplacements et la correspondance entre les attributs Peer_Adr et Adr_Served. Il ne contient que les adresses de destination.

E.4 NLSP en mode connexion

E.4.1 Fonctionnement de base

La complexité du protocole NLSP tient, pour l'essentiel, au traitement de l'établissement de la connexion pour les communications en mode connexion.

Tableau E.1

Emplacement	Param_Prot	Adresse NLSP	Adresse UN	Adresse NLSP/UN
A	FAUX	Adresse NSAP	Adresse NSAP	Identique
A	VRAI	Adresse NSAP	Adresse UN homologue	Différente
B: Système d'extrémité	FAUX	Adresse NLSP (voir Note)	Adresse UN homologue	Identique
B: Système d'extrémité	VRAI	Adresse NLSP (voir Note)	Adresse UN homologue	Différente
B: Système intermédiaire	FAUX	Adresse NLSP (voir Note)	Adresse UN homologue	Identique
B: Système intermédiaire	VRAI	Adresse NLSP (voir Note)	Adresse UN homologue	Différente
NOTE – La mise en correspondance de l'adresse NLSP avec l'adresse NSAP et vice versa relève des fonctions de routage relatives au protocole situé au-dessus du NLSP.				

Deux modes fondamentaux d'établissement de la connexion NLSP sont mis en œuvre. Dans le premier, les paramètres NLSP-CONNECT sont acheminés dans les primitives de service UN-CONNECT. Dans le second, les paramètres NLSP-CONNECT sont, après avoir été encapsulés dans une SDT PDU, acheminés dans une primitive UN-DATA après l'établissement de la connexion UN. Il existe des variantes de ces deux modes d'établissement de connexion NLSP dont une est utilisée avec un protocole SA-P dans la bande et l'autre avec une association SA qui a été établie hors bande.

La PDU de «commande de sécurité de connexion» (CSC) (*connection security control*) est utilisée pour signaler le mode d'établissement de la connexion et, si le protocole SA-P dans la bande n'est pas acheminé dans la connexion UN, l'échange de CSC PDU est également utilisé pour:

a) établir des attributs de sécurité spécifiques des mécanismes qui doivent être utilisés pour protéger la connexion (par exemple, clés, numéros de séquence d'intégrité);

b) assurer l'authentification de l'entité homologue.

Dans le cas où le paramètre NLSP-CONNECT est acheminé dans une primitive UN-CONNECT avec protocole SA-P dans la bande, une connexion UN est établie pour acheminer le protocole SA-P puis est libérée avant l'échange de primitives UN-CONNECT acheminant les paramètres NLSP-CONNECT. Les CSC PDU sont utilisées lors du deuxième échange de primitives UN-CONNECT pour une nouvelle authentification des entités NLSP homologues.

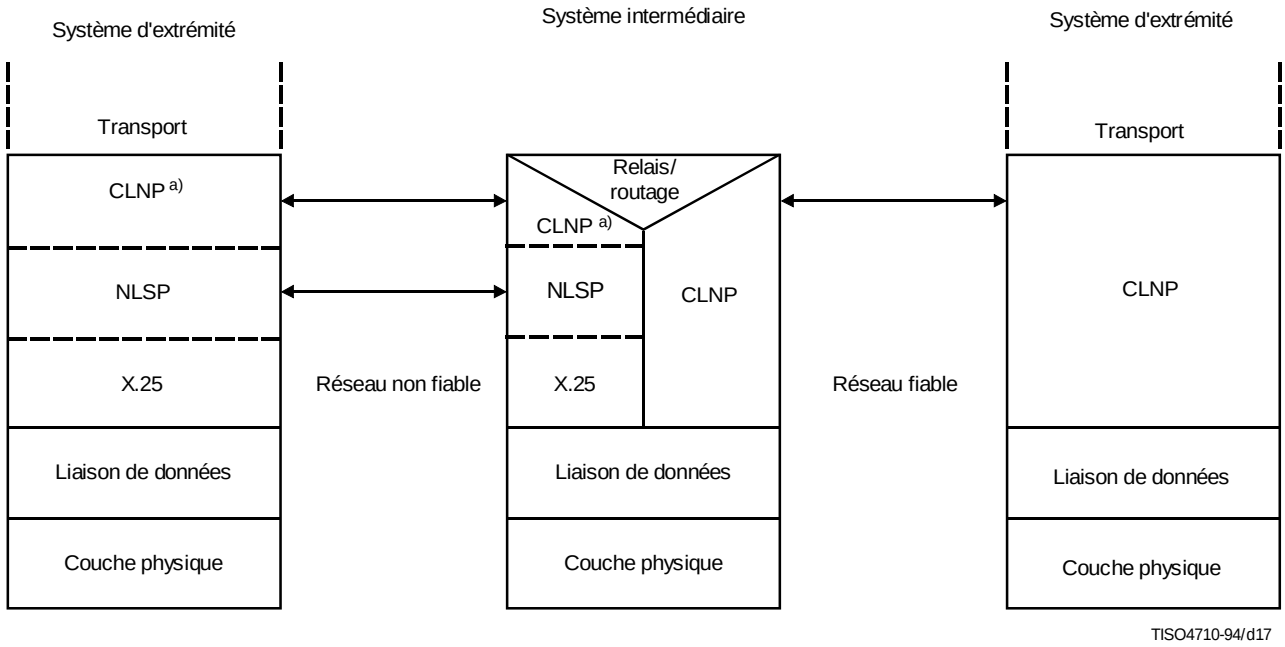
L'établissement de l'association SA est effectué par l'échange de SA PDU ou SDT PDU qui acheminent les informations nécessaires pour établir les attributs SA requis. L'Annexe C définit un protocole SA à cet effet.

Si les paramètres NLSP-CONNECT doivent être protégés, ils seront encapsulés dans une SDT PDU ou codés (sélection du mode No_Header) avant leur transfert.

Une fois qu'une connexion a été établie, les données d'utilisateur sont protégées par encapsulation dans une SDT PDU ou, si le mode No_Header est sélectionné, par simple codage des données d'utilisateur NLSP.

E.4.2 Emplacement

Le protocole NLSP en mode connexion peut être placé à divers endroits de la couche réseau. Il fournit à l'utilisateur NLSP une interface de service de réseau OSI (dans ce cas, l'utilisateur correspond à une entité de transport) ou, si l'utilisateur est une entité de protocole de réseau additionnelle (par exemple, CLNP de la Rec. UIT-T X.233 | ISO/CEI 8473), le service correspond à une interface de sous-réseau. L'interface au-dessous du protocole NLSP est virtuellement identique à celle du service de réseau OSI, sauf que l'utilisateur du service est le protocole NLSP au lieu du service de transport et que le service peut fonctionner dans un système d'extrémité ou un système intermédiaire. Le protocole situé au-dessous du protocole NLSP se comporte comme s'il fonctionnait entre deux systèmes d'extrémité assurant le service de réseau OSI bien que, dans une optique générale, il puisse fonctionner seulement avec un système intermédiaire et ne soit pas directement relié au service de transport. La mise en œuvre du protocole NLSP-CO avec un système intermédiaire et de bout en bout est illustrée sur les Figures E.4-1, E.4-2, E.4-3 et E.4-4. D'autres emplacements du protocole NLSP sont possibles.



a) NOTE – Y compris la fonction de convergence avec le mode CO.

Figure E.4-1 – Illustration du protocole NLSP dans un environnement multiréseau

E.4.3 Mise en correspondance des interfaces de service NLSP/UN

Dans un système d'extrémité, l'interface de service NLSP est mise directement en correspondance avec le service de réseau OSI.

Deux formes de mise en correspondance du service UN sont possibles. Dans la première, l'interface de service UN est mise en correspondance avec le service de réseau OSI équivalent, la CSC PDU étant acheminée dans le champ données d'utilisateur UN-CONNECT. Dans la seconde, le service UN est mis directement en correspondance avec la Recommandation X.25, comme indiqué dans la Rec. X.223 du CCITT | ISO 8878, sauf que la CSC PDU est acheminée dans le champ «services complémentaires de protection» de la Recommandation X.25.

E.4.4 Adressage

Les adresses utilisées à l'interface de service NLSP sont les adresses NSAP du service de réseau OSI si le protocole NLSP fonctionne à la partie supérieure de la couche réseau ou les adresses SNPA s'il fonctionne sous un autre protocole de couche réseau tel que le CLNP. S'il n'y a pas dissimulation d'adresse (c'est-à-dire si l'attribut Param_Prot est FAUX), les adresses à l'interface de service UN sont les mêmes que celles à l'interface de service NLSP.

Si la dissimulation des adresses est assurée (c'est-à-dire si l'attribut Param_Prot est VRAI), les adresses utilisées à l'interface de service UN (adresses UN) sont de la même forme que les adresses NLSP (par exemple, dans le cas où l'adresse NLSP est une adresse NSAP structurée conformément à la Rec. X.213 du CCITT | ISO 8348/AD2), mais elles servent à identifier des entités NLSP qui peuvent être situées dans un système intermédiaire ou d'extrémité. Ces adresses UN peuvent être gérées de la même manière que les adresses NSAP. Les mêmes systèmes d'enregistrement peuvent être utilisés pour attribuer les adresses et les mêmes protocoles de routage peuvent être utilisés pour gérer le routage. Cependant, ces adresses sont situées dans des domaines de routage isolés. La mise en correspondance de l'adresse NSAP avec l'adresse UN est traitée par le protocole NLSP qui utilise l'attribut d'association de sécurité Adr_Served pour identifier l'adresse NSAP desservie par les adresses UN contenues dans l'attribut d'association de sécurité Peer_Adr.

E.5 NLSP en mode sans connexion

E.5.1 Fonctionnement de base

La protection du protocole NLSP-CL est assurée par simple encapsulation des données d'utilisateur dans une SDT PDU.

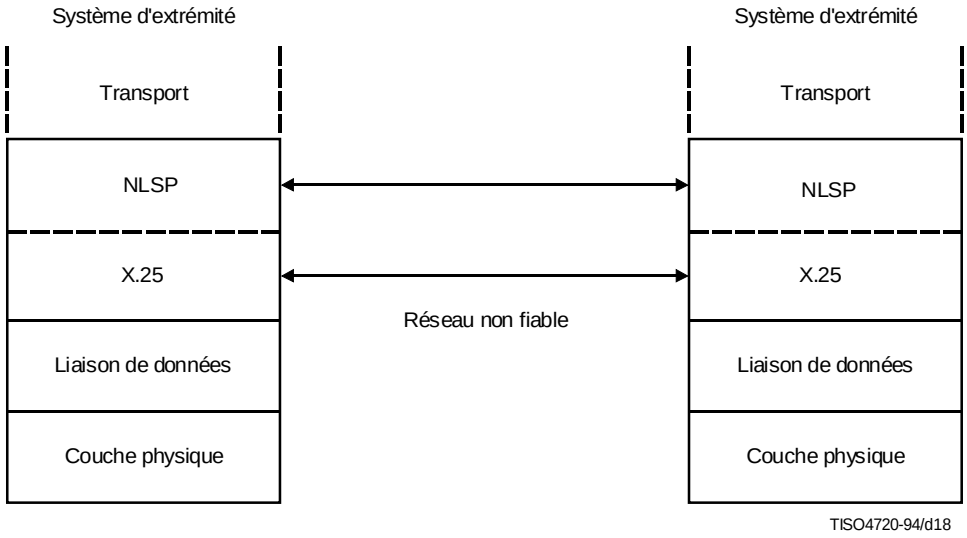


Figure E.4-2 – Ilustration du protocole NLSP-CO entre systèmes d'extrémité

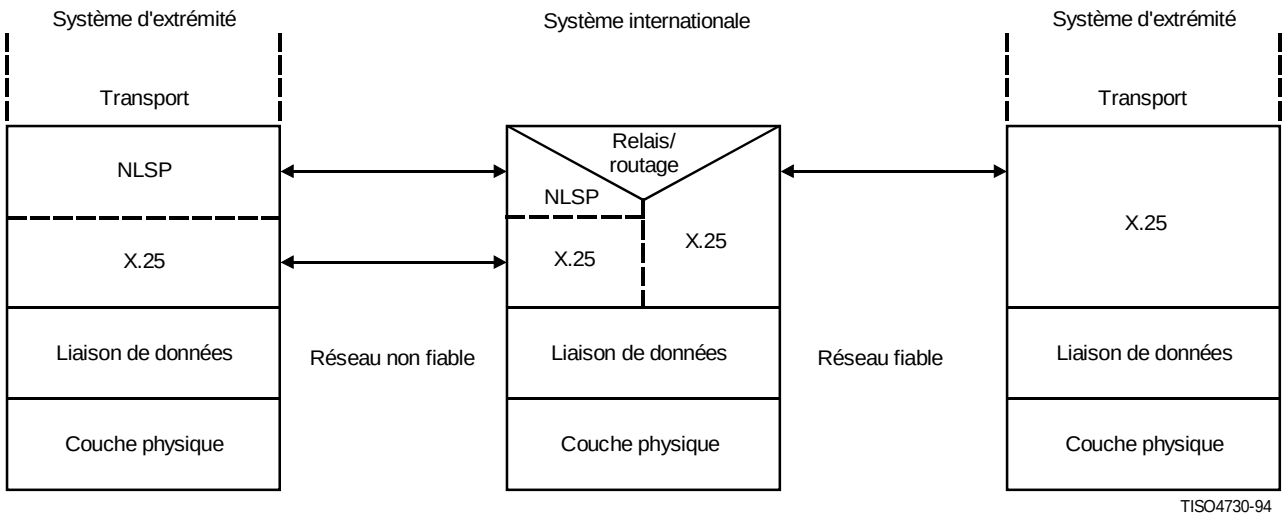


Figure E.4-3 – Protocole NLSP-CO avec un réseau non fiable

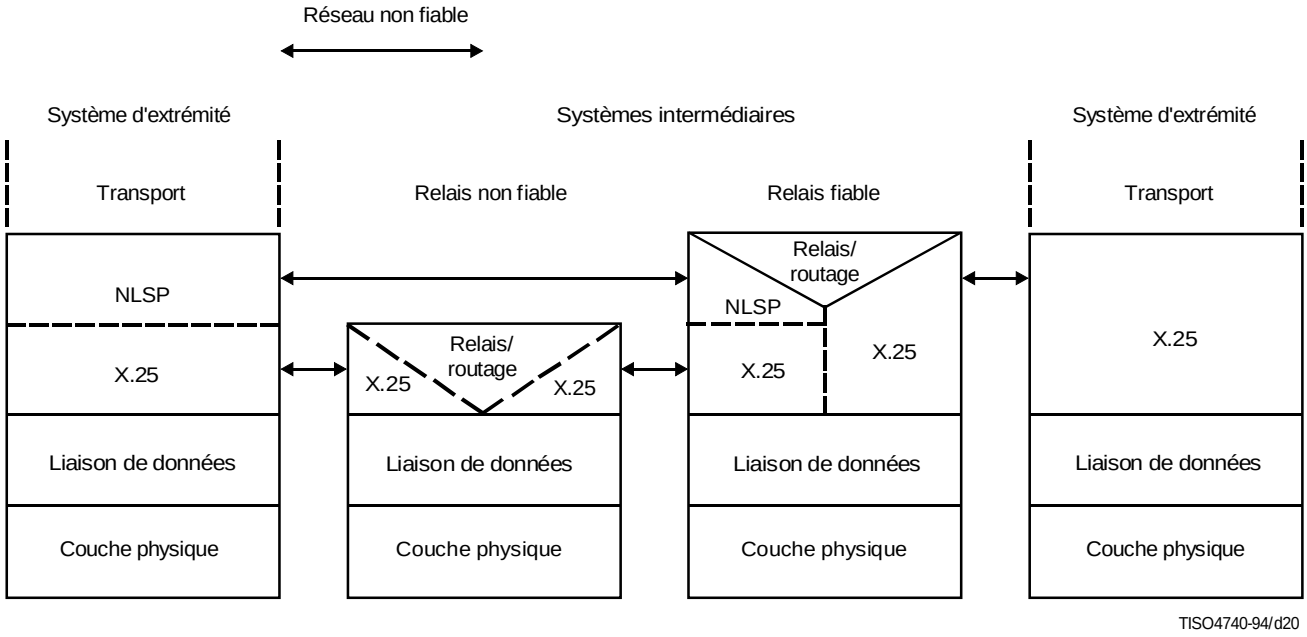


Figure E.4-4 – Illustration du protocole NLSP-CO avec système-relais non fiable

E.5.2 Emplacement

Le protocole NLSP pour le mode sans connexion peut:

a) fonctionner en haut de la couche réseau; il encapsule les NSDU dans une SDT PDU avant qu'elles soient traitées par le protocole de réseau en mode sans connexion (Rec. UIT-T X.233 | ISO/CEI 8473) (voir la Figure E.5-1). Cet empilement ne peut être utilisé qu'entre deux systèmes d'extrémité; ou

b) fonctionner au-dessous du protocole de réseau en mode sans connexion; il encapsule les PDU de protocole en mode sans connexion avant qu'elles soient mises en correspondance avec le sous-réseau de base (voir la Figure E.5-2). Cet empilement est utilisé conjointement avec les systèmes intermédiaires relais «fiables» ou de bout en bout lorsqu'il n'y a aucun relais de réseau entre deux systèmes communicants; ou

c) fonctionner sous une couche de protocole de la Rec. UIT-T X.233 | ISO/CEI 8473 (CLNP) pour le domaine «fiable/rouge» et être mis en correspondance avec une autre couche de protocole CLNP pour le domaine «non fiable/noir». Cet empilement est le plus souple et peut fonctionner dans n'importe quel environnement. Les systèmes intermédiaires «fiables» retransmettent le protocole CLNP supérieur après avoir supprimé la protection de sécurité assurée par le protocole NLSP. D'autres systèmes relais «non fiables» retransmettent le protocole CLNP inférieur en laissant passer en transparence les données NLSP protégées (voir la Figure E.5-3).

NOTES

1 La représentation de deux couches de la Rec. UIT-T X.233 | ISO/CEI 8473 et d'une couche NLSP n'implique pas nécessairement des machines de protocole distinctes. Le choix dépend de la politique de mise en œuvre locale.

2 L'existence de deux couches de protocole CLNP n'implique pas nécessairement des mises en œuvre distinctes.

E.5.3 Mise en correspondance des interfaces de service NLSP/UN

Dans le premier cas où le protocole NLSP fonctionne en haut de la couche réseau, l'interface de service NLSP est identique à celle du service de réseau OSI et l'interface de service UN est la même, sauf qu'elle est reliée à une entité NLSP plutôt qu'au service de transport.

Dans le deuxième cas où le NLSP fonctionne au-dessous du protocole CLNP, l'interface de service NLSP est équivalente au service assuré par un sous-réseau fonctionnant au-dessous du protocole CLNP et le service UN est le même que le service de sous-réseau.

Dans le dernier cas, l'interface au-dessus du protocole NLSP fonctionne vis-à-vis du protocole CLNP au-dessus comme s'il était un sous-réseau. Pour le protocole CLNP au-dessous, l'interface UN se comporte comme si elle était une interface du service de réseau OSI.

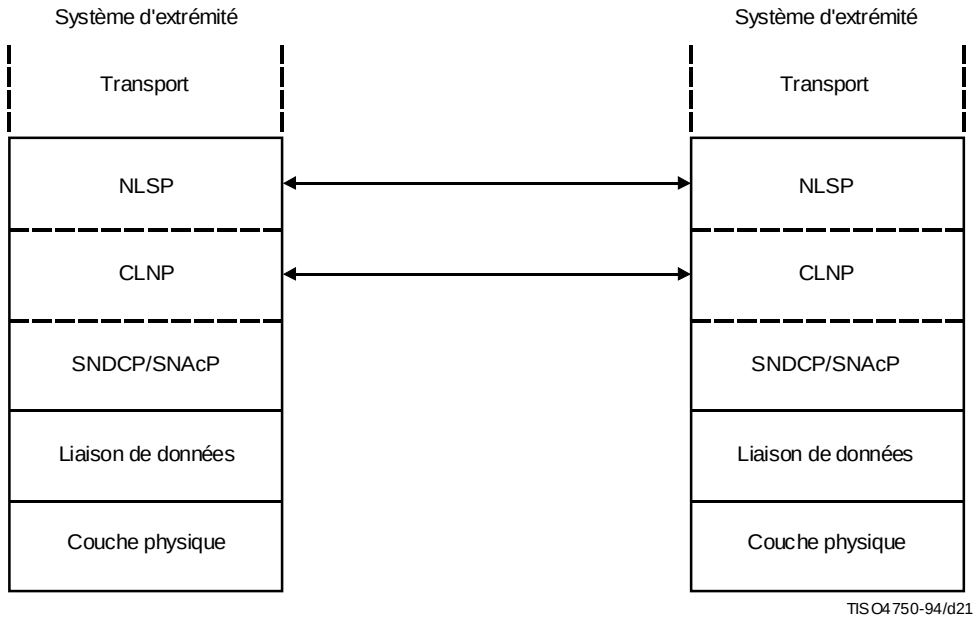


Figure E.5-1 – Illustration d'un protocole NLSP-CL entre système d'extrémité

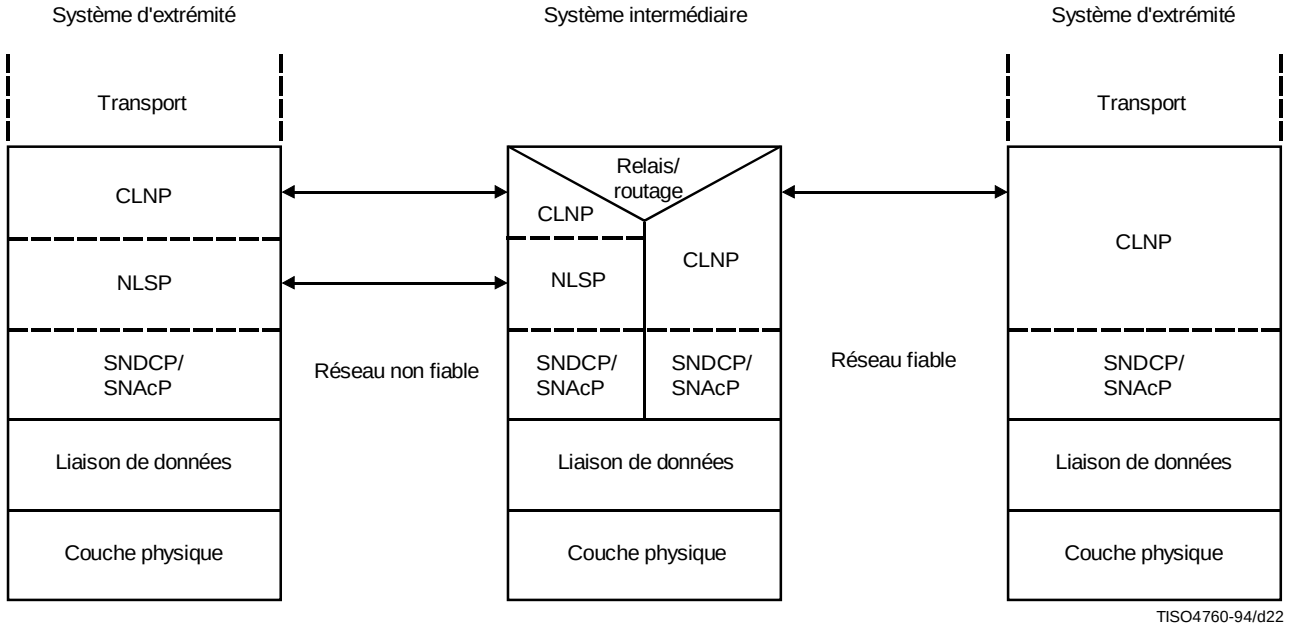


Figure E.5-2 – Illustration d'un protocole NLSP-CL avec sous-réseau non fiable

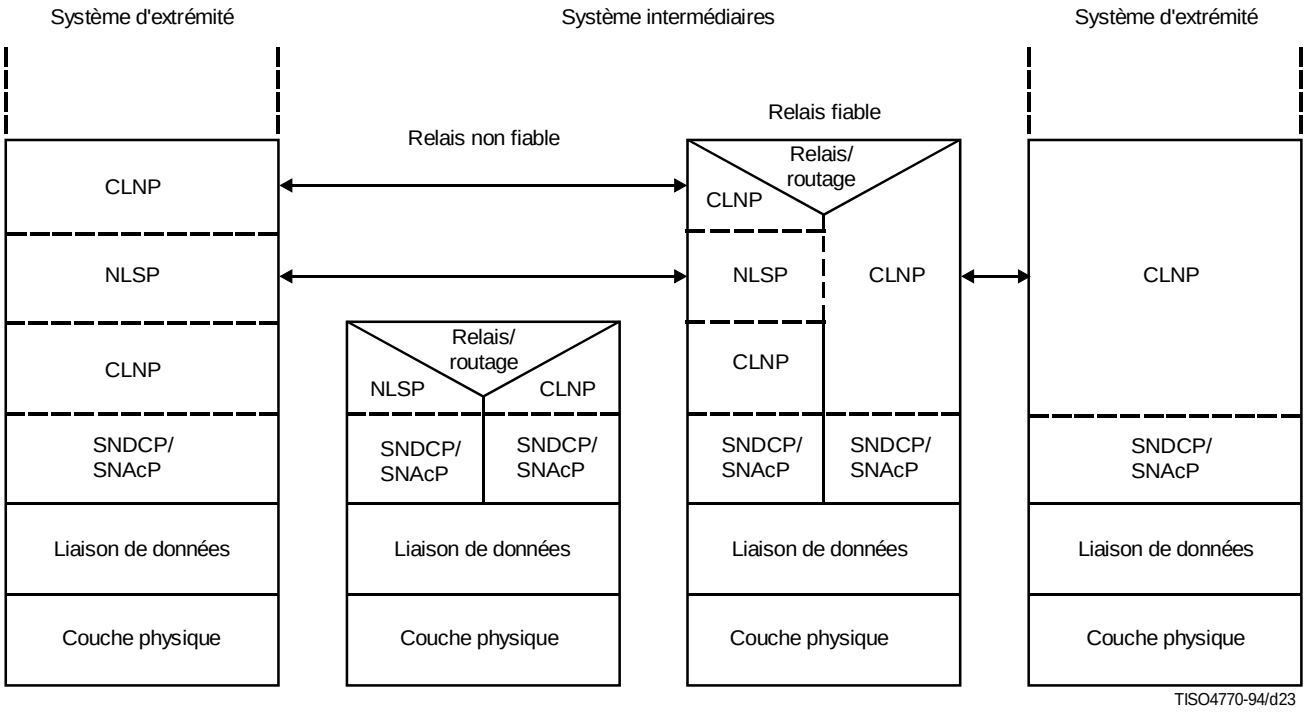


Figure E.5-3 – Illustration d'un protocole NLSP-CL avec système relais non fiable

E.5.4 Adressage

Dans le cas du protocole NLSP fonctionnant en haut de la couche réseau, l'adresse utilisée par le NLSP est une adresse NSAP de réseau OSI. Dans le cas du protocole NLSP fonctionnant au-dessous de la couche réseau (Rec. UIT-T X.233 | ISO/CEI 8473) (CLNP) avant d'être mis en correspondance avec le sous-réseau de base, l'adresse utilisée à l'interface au-dessus et au-dessous du protocole NLSP est une adresse de sous-réseau (par exemple, adresse MAC de réseau local). Dans le cas du protocole NLSP fonctionnant entre deux couches de protocole CLNP, l'adresse transmise à l'entité NLSP au-dessous est une adresse de sous-réseau.

S'il n'y a pas dissimulation d'adresse (c'est-à-dire si l'attribut Param_Prot est FAUX), les adresses utilisées à l'interface de service UN sont les mêmes que celles à l'interface de service NLSP.

Si la dissimulation d'adresse est mise en œuvre (c'est-à-dire si l'attribut Param_Prot est VRAI), les adresses utilisées à l'interface de service UN (adresses UN) sont de la même forme que les adresses NLSP, mais elles servent à identifier des entités NLSP qui peuvent être situées dans un système intermédiaire ou d'extrémité. Ces adresses UN peuvent être gérées de la même manière que les adresses NSAP. Les mêmes systèmes d'enregistrement peuvent être utilisés pour attribuer des adresses et les mêmes protocoles de routage peuvent être utilisés pour gérer le routage. Cependant, ces adresses sont situées dans des domaines de routage isolés. La mise en correspondance de l'adresse NSAP avec l'adresse UN est traitée par le protocole NLSP qui utilise l'attribut d'association de sécurité Adr-served pour identifier l'adresse NSAP desservie par les adresses UN contenues dans l'attribut d'association de sécurité Peer_Adr.

E.5.5 Segmentation

La segmentation et le réassemblage sont traités par la Rec. UIT-T X.233 | ISO/CEI 8473 (CLNP). La segmentation peut avoir lieu avant et après le traitement NLSP selon les sous-réseaux de base que la PDU a traversés. Si la segmentation a lieu avant le protocole NLSP, chaque segment est encapsulé par le protocole NLSP, envoyé au dispositif de décapsulation du NLSP, décapsulé puis réassemblé par le protocole CLNP. Si la segmentation a lieu après le protocole NLSP, le protocole CLNP réassemblera d'abord les segments. La PDU complète sera décapsulée par le protocole NLSP. Le protocole CLNP livrera la PDU décapsulée à l'adresse de destination indiquée à l'aide des protocoles de communication normaux.

E.6 Attributs et associations de sécurité

Les deux protocoles NLSP-CO et NLSP-CL nécessitent un ensemble d'attributs correspondants, appelés attributs d'association de sécurité, pour que des communications sûres puissent être établies. Il s'agit notamment des attributs suivants:

a) informations relatives à la «politique» de base qui définissent ou restreignent le fonctionnement du protocole NLSP (par exemple, algorithme de codage, longueur du bloc de codage, longueur du numéro de séquence d'intégrité, autorité qui définit les étiquettes);

b) valeurs initiales nécessaires pour commander la mise en œuvre du protocole NLSP (par exemple, clés maîtresses, numéros de séquence d'intégrité initiaux);

c) valeurs applicables nécessaires pour commander le fonctionnement du protocole NLSP (clé active pour une connexion particulière, numéro de séquence d'intégrité applicable).

Un ensemble d'attributs correspondants est appelé association de sécurité. L'ensemble d'attributs utilisé pour protéger une PDU en mode sans connexion ou une connexion est référencé par un identificateur d'association de sécurité.

Le premier ensemble d'informations relatives à la «politique» est appelé ensemble agréé de règles de sécurité (ASSR) (*agreed set of security rules*). Il est suggéré d'établir cet ensemble par enregistrement.

Le deuxième ensemble d'informations initiales de commande peut être établi hors bande à l'aide d'une interface de gestion locale ou d'un système de gestion OSI, ou dans la bande à l'aide d'un protocole appelé protocole d'établissement d'association de sécurité qui fonctionne conjointement avec le protocole NLSP.

Le troisième ensemble d'informations est mis à jour dans le cadre du fonctionnement du protocole NLSP de base. Par exemple, des clés actives peuvent être établies dans le protocole NLSP-CO par l'échange de PDU de commande de sécurité de connexion; les numéros de séquence d'intégrité applicables sont mis à jour dans chaque PDU de transfert de données sûres.

E.7 Relation fonctionnelle dynamique entre protocoles NLSP et CLNP

E.7.1 Introduction

Le paragraphe E.5.2 décrit la relation entre les protocoles NLSP et CLNP pour une instance de communication. Le but de ce paragraphe est de démontrer la souplesse du protocole NLSP utilisé conjointement avec le protocole CLNP pour établir des communications protégées et non protégées indépendantes de l'architecture des communications.

La Figure E.7-1 décrit le flux de données à l'entrée et à la sortie de ces protocoles combinés. Le texte qui suit décrit ce flux de données et les paramètres de communication qu'il nécessite.

E.7.2 Indication SN-UNITDATA

a) Lors d'une indication SN-UNITDATA (1) [Rec. UIT-T X.233 | ISO/CEI 8473 (CLNP) (voir 5.5)], l'identificateur de protocole (PID) dans le premier octet (ou, si l'adressage est utilisé pour identifier le protocole, l'adresse) est vérifié pour déterminer si la première partie de la PDU contient un en-tête CLNP ou NLSP (2).

b) Si le premier en-tête identifie le protocole CLNP, une décision est prise en fonction de l'adresse de destination dans l'en-tête CLNP (3). Si l'adresse de destination est reconnue en tant qu'adresse de système d'extrémité propre au protocole CLNP, la CLNP PDU est envoyée au processus de réassemblage (4) [CLNP (voir 6.8)]. S'il ne s'agit pas de l'une des adresses du système d'extrémité, l'en-tête CLNP est traité pour retransmission (8) comme indiqué au E.6.4.

c) Si le premier en-tête identifie le protocole NLSP, les paramètres de service de sous-réseau et les données d'utilisateur sont traités par le protocole NLSP comme un paramètre UN-UNITDATA. L'indication d'utilisateur NLSP-UNITDATA qui en résulte est alors vérifiée pour déterminer si le premier octet est un identificateur CLNP PID (8). Dans l'affirmative, le paramètre NLSP-UNITDATA est traité comme en b) ci-dessus (3); dans le cas contraire, l'indication NLSP-UNITDATA est mise en correspondance avec l'indication N-UNITDATA (7).

d) Après réassemblage par le protocole CLNP (si nécessaire) (4), une autre décision est nécessaire (5). Si la CLNP PDU contient une NLSP PDU (c'est-à-dire si le premier octet contient l'identificateur NLSP PID), les paramètres de service CLNP et les données d'utilisateur sont traités par le protocole NLSP comme une indication UN-UNITDATA (6); dans le cas contraire, ils sont mis directement en correspondance avec une indication N-UNITDATA (7). L'indication d'utilisateur NLSP-UNITDATA qui en résulte est

alors vérifiée pour déterminer si le premier octet est un identificateur CLNP PID (8) (ou, si l'adressage est utilisé pour identifier le protocole, l'adresse est vérifiée). Dans l'affirmative, le paramètre NLSP-UNITDATA est traité comme en b) ci-dessus (3); dans le cas contraire, l'indication NLSP-UNITDATA est mise en correspondance avec l'indication N-UNITDATA (7).

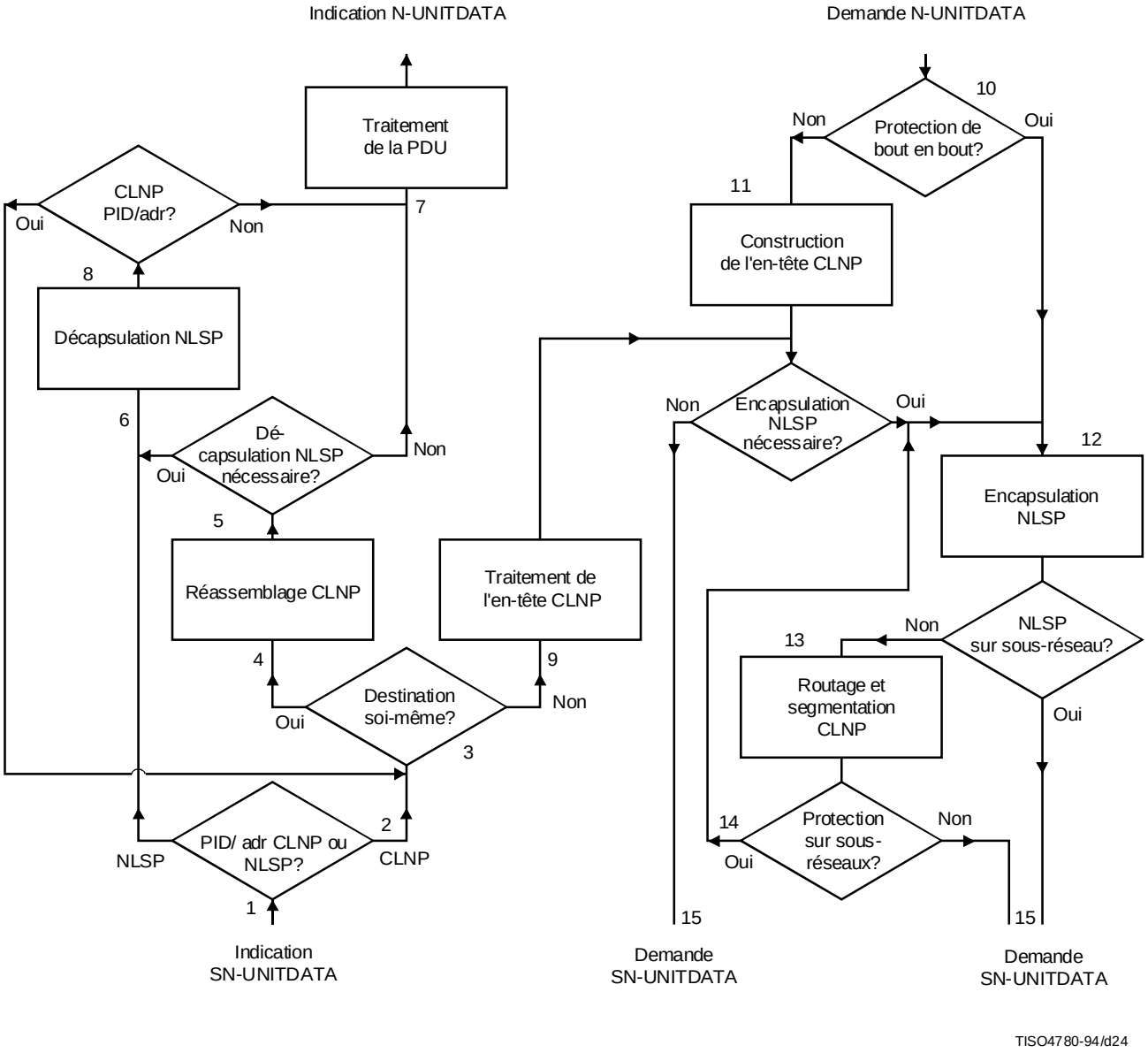


Figure E.7-1 – Organigramme de fonctionnement du NLSP avec le CLNP

E.7.3 Demande N-UNITDATA

a) Lors d'une demande N-UNITDATA (10), selon les paramètres de service (par exemple, adresse d'origine, de destination) et la politique de sécurité locale, la demande est mise directement en correspondance avec le protocole CLNP (voir 5.4) (11) ou avec une demande NLSP-UNITDATA et est traitée en conséquence (12).

b) Si le paramètre N-UNITDATA est traité par le protocole CLNP (11), la CLNP PDU qui en résulte est mise directement en correspondance avec une demande SN-UNITDATA (15) ou une demande NLSP-UNITDATA (10) pour traitement par le protocole NLSP.

c) Si le paramètre N-UNITDATA ou une CLNP PDU sont traités par le protocole NLSP (12), la demande UN-UNITDATA qui en résulte est mise directement en correspondance avec la demande SN-UNITDATA (15) ou avec le protocole CLNP pour traitement, comme s'il s'agissait d'un paramètre N-UNITDATA (13), en fonction des paramètres de service et de la politique de sécurité locale. Après traitement par le protocole CLNP, une protection supplémentaire peut être assurée par le protocole NLSP si elle est nécessaire sur le sous-réseau (14), sinon la CLNP PDU est mise en correspondance avec le paramètre SN-UNITDATA.

E.7.4 Envoi d'une CLNP PDU

La décision de protéger une CLNP PDU envoyée est fondée sur les informations contenues dans l'en-tête de la CLNP PDU et les données d'utilisateur ainsi que sur la politique de sécurité locale. Si une protection est nécessaire, la CLNP PDU est mise en correspondance avec une demande NLSP-UNITDATA pour traitement par le protocole NLSP (12). Selon les paramètres de service et la politique de sécurité locale, le paramètre UN-UNITDATA protégé qui en résulte est mis directement en correspondance avec une demande SN-UNITDATA [CLNP (voir 6.5)] (15) ou avec le protocole CLNP pour traitement, comme s'il s'agissait d'un paramètre N-UNITDATA (13), en fonction des paramètres de service et de la politique de sécurité locale.

E.7.5 Récapitulation des interfaces CLNP/NLSP-CL

Les paragraphes qui précèdent indiquent la relation fonctionnelle entre protocole NLSP-CL et protocole CLNP. Pour des raisons de simplicité, ces protocoles sont présentés comme des systèmes distincts séparés par des interfaces de service. Les deux protocoles peuvent être mis en œuvre comme un seul protocole de couche 3 combinant les fonctions des machines de protocole CLNP et NLSP.

E.8 Fonctions dynamiques liées au modèle structuré en couches

L'organigramme qui énumère les opérations effectuées dans l'exemple de configuration présenté sur la Figure E.7-2 correspond à la structure en couches utilisée ci-dessus pour décrire le protocole NLSP.

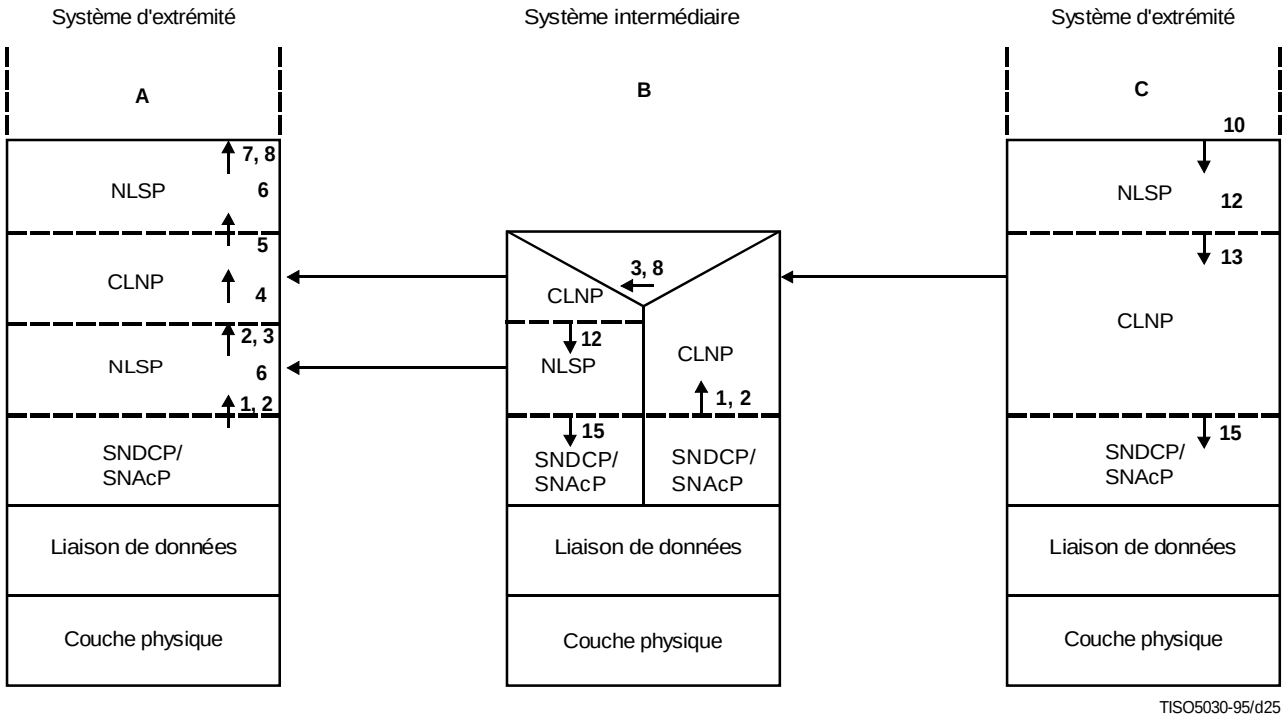


Figure E.7-2 – Modèle en couches correspondant à l'organigramme ci-après

Action	Organigramme – Référence
Dans le système d'extrémité A	
Indication SN-UNITDATA dans système d'extrémité C	1
Vérification si CLNP ou NLSP	2
Vérification si destination locale	3
Réassemblage CLNP	4
Vérification si NLSP	5
Mise en correspondance UN-UNITDATA et désencapsulation NLSP	6
Mise en correspondance avec indication N-UNITDATA	7
Vérification si CLNP	8
Dans le système intermédiaire B	
Indication SN-UNITDATA dans système intermédiaire B	1
Vérification si CLNP ou NLSP	2
Vérification si destination locale	3
Traitement CLNP pour envoi	8
Mise en correspondance NLSP-UNITDATA et encapsulation NLSP	12
Mise en correspondance UN-UNITDATA avec demande SN-UNITDATA	15
Dans le système d'extrémité C	
Demande N-UNITDATA dans système d'extrémité A	10
Mise en correspondance NLSP-UNITDATA et encapsulation NLSP	12
Mise en correspondance UN-UNITDATA avec CLNP pour traitement comme N-UNITDATA	13
Mise en correspondance CLNP PDU avec demande SN-UNITDATA	15

Annexe F

Exemple d'ensemble agréé de règles de sécurité

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

Un ensemble agréé de règles de sécurité (ASSR) établit les mécanismes de sécurité, y compris tous les paramètres nécessaires qui doivent être utilisés pour définir le fonctionnement des mécanismes, pour un service de sécurité sélectionné. La présente annexe donne un exemple de la façon dont les valeurs des attributs SA susceptibles d'être établis par un ensemble ASSR pourraient être indiquées sur un formulaire.

ASSR-ID XYZ(Object identifier) -- *Indique la référence d'objet utilisée dans le SA-P.*

SA-ID_Length 4

Security services selected Definition Module -- *Indique les services de sécurité qui pourraient être mis en œuvre dans le cadre des règles de sécurité et donne des noms aux niveaux de protection assurés à l'aide de différents algorithmes, différentes longueurs de clé, etc.*

PE Auth:	**none,**	**low,**	**high**
AC:	**none,**	**low,**	**high**
Confid:	**none,**	**low,**	**high**
Integ:	**none,**	**low,**	**high**

Security Label Mapping -- *Mise en correspondance des étiquettes de sécurité avec les sélections de services de sécurité.*

Label_Def_Auth XYZ

Label->Sensitivity = Unclass
implies:
PE Auth none, AC none, Confid none, Integ none

Label-Sensitivity = Confidential
implies:
PE Auth low, AC low, Confid low, Integ none

Label-Sensitivity = Secret
implies:
PE Auth high, AC high, Confid high, Integ high

Param_Prot TRUE -- *Mise en correspondance des étiquettes de sécurité avec les sélections de services de sécurité.*

For Security services selected: Integ = high or Conf = high

Mechanism Module – Security labels for Access Control
For Security services selected: AC = high or Conf = high
-- *Sélection des niveaux de protection qui nécessitent la protection de tous les paramètres de service.*

Label_Def_Auth XYZ
(Note this must be the same as Auth for protection QOS labels)

Explicit indication Yes

Mechanism Module – Integrity Check Value
For security service selection: Integ > none or PE Auth = High or Mechanism Security Labels

ICV_Alg XYZ
Rekey after 10 000 PDUs
Key distrib mechanism Asymmetric

Mechanism Module – Integrity Sequence Number

For security services selected: Integ = high or Auth = High

ISN_Len	**8 octets total**
Sequence Number	**4 octets**
incremented by 1	
Timestamp	**4 octets**
milliseconds from sync point	
Receive ISN Window	**Discard previous sequence #.**
Timestamp should be within 2*maximum	
variation in network	
delay. If outside	
window then a replay attack.	

Mechanism Module – Encipherment

For security services selected: Conf > low

Enc_Alg_ID	**XYZ**
Mode Chained	
Enc_Blk	**8 octets**
key exchange info	**(e.g. Prime p, Generator a)**
Rekey after	**1 000 PDUs**
Key distrib mechanism	**Asymmetric**

Mechanism Module – No Header

For security services selected: Conf = low and Integ = none and not Label mechanism

Mechanism Module – Connection Authentication

For security services selected: AC > Low or PE Auth > Low

Enc_Alg_ID	**XYZ**

Mechanism Module – Asymmetric Key Distribution

For mechanism encipherment or Integrity check value

Enc_Alg	**RSA**

Annexe G

Associations et attributs de sécurité

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

Pour protéger une instance de communication (une SDU en mode sans connexion ou une connexion), un ensemble d'informations (clés et autres attributs nécessaires pour commander le fonctionnement de la sécurité) doit être établi entre les entités communicantes. Cet ensemble d'informations est appelé association de sécurité (SA) (*security association*).

Les informations qui forment une association SA sont soit des informations statiques qui peuvent être «personnalisées» lorsque l'association SA est établie puis restent fixes pendant la durée de l'association, soit des informations dynamiques qui peuvent être mises à jour pendant la durée de l'association de sécurité.

Une association SA peut être établie hors bande ou, pour le protocole NLSP-CO, dans la bande par l'échange de SA PDU. Lorsqu'on applique la méthode dans la bande, les mécanismes particuliers utilisés pour mettre en œuvre le protocole SA-P peuvent être tels que ceux définis dans la présente Recommandation de l'UIT-T | Norme internationale ou peuvent être des mécanismes privés.

Avant d'établir une association SA, chaque entité NLSP doit avoir préétabli:

a) un ensemble commun de règles de sécurité qui, en fonction d'un service de sécurité choisi, spécifie les mécanismes de sécurité à utiliser, y compris tous les paramètres nécessaires pour définir le fonctionnement des mécanismes (par exemple, algorithme, longueur de clé, durée de la clé). Ces règles de sécurité sont mutuellement convenues et identifiées de manière unique par les entités communicantes. Les règles de sécurité et leurs identificateurs peuvent être enregistrés par des tiers. Voir l'Annexe F pour un exemple d'ensemble de règles de sécurité;

b) les services de sécurité, donc les mécanismes de sécurité, qui peuvent être utilisés.

Si on utilise la méthode d'établissement d'une SA dans la bande, les éléments suivants doivent être préétablis:

c) les services de sécurité initialement sélectionnés, donc les mécanismes de sécurité à utiliser pour établir l'association SA;

d) les informations de clé de base nécessaires pour établir une association SA.

Lors de l'établissement de la SA, une entité NLSP établit les informations suivantes partagées avec son entité homologue distante:

e) identificateurs SA-ID local et distant;

f) services de sécurité qui doivent être utilisés entre les entités associées pour les instances de communication;

g) mécanismes et leurs paramètres résultant implicitement des services de sécurité sélectionnés;

h) clés initiales partagées pour les mécanismes d'intégrité, de codage et l'authentification d'une instance de communication;

i) ensemble d'étiquettes de sécurité et d'adresses qui peuvent être utilisées dans cette association pour le contrôle d'accès.

Les références SA et les clés partagées [points e) et h) ci-dessus] doivent être établies association par association. Les autres informations peuvent être préétablies et être communes à plusieurs associations. En outre, dans le cadre de l'établissement d'une association SA personnalisée, l'identité de l'entité homologue distante doit être authentifiée. L'Annexe C définit un mécanisme qui peut être utilisé pour la répartition de clés et l'authentification.

Les informations suivantes peuvent être mises à jour dynamiquement pour une instance de communication:

j) numéro(s) de séquence d'intégrité nécessaire(s) pour les données normales et exprès dans chaque sens;

k) étiquette de sécurité;

l) informations de nouveau codage pour les mécanismes de codage/d'intégrité.

Pour réaliser l'authentification, des mécanismes d'authentification doivent être appliqués à chaque instance de communication.

Les différents attributs SA qui peuvent être établis aux différents stades d'une association de sécurité sont illustrés sur la Figure G.1.

<table>
<tr><th>Préétabli</th><th>Statique</th><th>Dynamique</th></tr>
<tr><td>Gamme de services de sécurité sélectionnés
Services de sécurité initiaux sélectionnés
Informations de clé de base
Ensemble convenu de règles de sécurité</td><td>Clés initiales
SA-ID
Authentification
Etiquette de sécurité</td><td>ISN
Authentification
SA-ID
Informations de nouveau codage</td></tr>
<tr><td colspan="2">Services de sécurité sélectionnés
Mécanismes sélectionnés
Ensemble d'étiquettes de sécurité/ensemble d'adresses</td><td></td></tr>
</table>

Figure G.1 – Illustration de trois stades d'association de sécurité

Annexe H

Exemple d'échange de jetons de clé – Algorithme EKE

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

Un exemple d'algorithme d'échange de jetons de clé qui peut être utilisé avec le protocole d'association de sécurité défini dans l'Annexe C est donné ci-après.

Deux paramètres sont nécessaires pour l'échange EKE. Le premier est un nombre premier p élevé (tel que p – 1 ait un facteur premier élevé) et le second est un nombre «a» inclus dans les limites $1 < a < p – 1$.

Soit A et B les deux entités communicantes (voir la Figure H.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 mod p) et envoie a, p et (a**X mod p) à B qui calcule la formule (a**Y mod p) et l'envoie à A. A et B calculent la formule (a**XY mod P). Seules les formules (a**X mod P) et (a**Y mod 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 mod p).

A et B peuvent utiliser ultérieurement comme clés des sous-ensembles des éléments binaires contenus dans la formule (a**XY mod P).

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

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

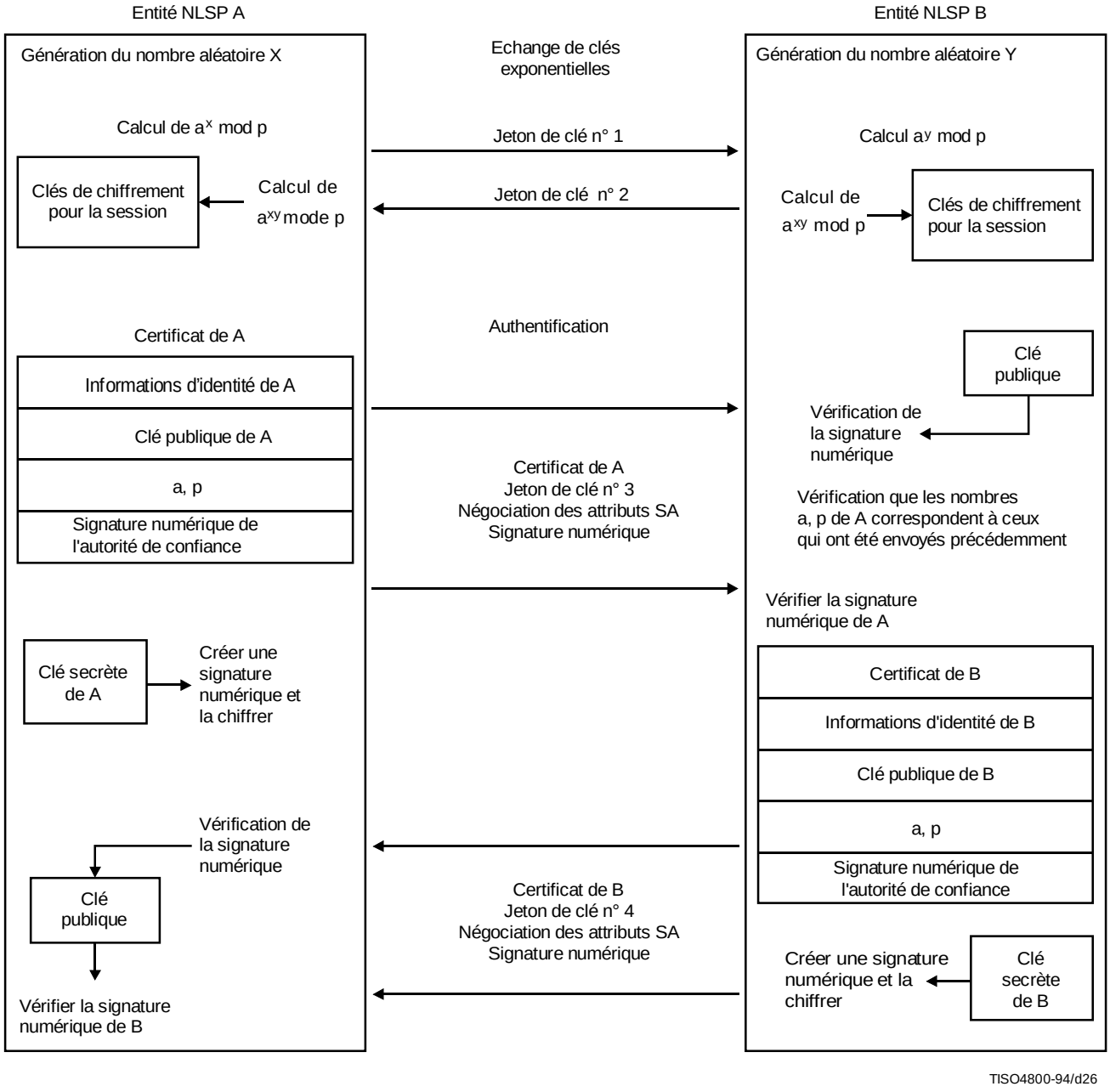


Figure H.1 – Illustration d'un calcul de clé en cours de communication et à l'aide d'un algorithme EKE