NORME INTERNATIONALE

ISO/CEI 11577

Première édition
1995-05-15

Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — Protocole de sécurité de la couche réseau

Information technology — Open Systems Interconnection — Network layer security protocol

Numéro de référence
ISO/CEI 11577:1995(F)

Sommaire

Version française tirée en 1996

Imprimé en Suisse

Avant-propos

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

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

La Norme internationale ISO/CEI 11577 a été élaborée par le comité technique mixte ISO/CEI JTC 1, *Technologies de l'information*, sous-comité SC 6, *Téléinformatique*, en collaboration avec l'IUT-T. Le texte identique est publié en tant que Recommandation IUT-T X.273.

NOTE — Les dates de publication de l'ISO/CEI 7498-1, l'ISO/CEI 9646-1, l'ISO/CEI 9646-2, l'ISO/CEI 10731, l'ISO/CEI 10745 et l'ISO/CEI TR 13594, auxquelles il est fait référence dans la présente Norme internationale, diffèrent de celles auxquelles il est fait référence dans la Recommandation IUT-T X.273, du fait de la publication de nouvelles éditions pendant la préparation finale de la présente Norme internationale.

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

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 DE SYSTÈMES OUVERTS (OSI) – PROTOCOLE DE SÉCURITÉ DE LA COUCHE RÉSEAU

1 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:—[1], *Technologie de l'information – Interconnexion de systèmes ouverts – Modèle de sécurité des couches inférieures.*
- Recommandation UIT-T X.803 (1994) | ISO/CEI TR 10745:—[1], *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/CEI 7498-1:1994, *Technologie de l'information – Interconnexion de systèmes ouverts – Modèle de référence de base: Le modèle de base.*

- 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.210 du CCITT (1993), *Technologie de l'information – Interconnexion de systèmes ouverts – Conventions pour la définition de services OSI.*

  ISO/CEI 10731:1994, *Technologie de l'information – Interconnexion de systèmes ouverts – Modèle de Référence de Base – Conventions pour la définition des services OSI.*

- 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 9646-1:1994, *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 9646-2:1994, *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.*

- 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.*

---

1) À publier.

2.3 Références additionnelles

- ISO/CEI 8208:1990, *Technologie de l'information – Communication de données – Protocole X.25 de couche paquets pour terminal de données.*
- ISO 8648:1988, *Systèmes de traitement de l'information – Communication de données – Organisation interne de la couche réseau.*
- 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 I Norme internationale utilise les termes suivants définis dans la Rec. X.210 du CCITT I ISO TR 8509:

a) fournisseur de service;

b) utilisateur de service.

3.4 Définitions du service de réseau

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

– point de rattachement au sous-réseau.

3.5 Définitions de l'organisation interne de la couche réseau

La présente Recommandation I 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 I Norme internationale utilise les termes suivants définis dans la Rec. UIT-T X.233 I 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 I Norme internationale utilise les termes suivants définis dans la Rec. UIT-T X.803 I ISO/CEI 10745:

a) politique d'interaction sûre;

b) relation de sécurité.

3.8 Définitions des tests de conformité

La présente Recommandation I Norme internationale utilise les termes suivants définis dans la Rec. X.290 du CCITT I 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 I 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 I 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 I ISO 10745.

3.9.10 étiquette: Voir «étiquette de sécurité» (Rec. X.800 du CCITT I 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);