NORME INTERNATIONALE

ISO 9735-7

Première édition
1999-08-01

Échange de données informatisé pour l'administration, le commerce et le transport (EDIFACT) — Règles de syntaxe au niveau de l'application (numéro de version de syntaxe: 4) —

Partie 7:

Règles de sécurité pour le lot EDI (confidentialité)

Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4) —

Part 7: Security rules for batch EDI (confidentiality)

Numéro de référence
ISO 9735-7:1999(F)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax. + 41 22 749 09 47
E-mail copyright@iso.ch
Web www.iso.ch

Version française parue en 2000

Imprimé en Suisse

Sommaire

Page

Avant-propos

L'ISO (Organisation internationale de normalisation) est une fédération mondiale d'organismes nationaux de normalisation (comités membres de l'ISO). L'élaboration des Normes internationales est en général confiée aux comités techniques de l'ISO. Chaque comité membre intéressé par une étude a le droit de faire partie du comité technique créé à cet effet. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO participent également aux travaux. L'ISO collabore étroitement avec la Commission électrotechnique internationale (CEI) en ce qui concerne la normalisation électrotechnique.

Les projets de Normes internationales adoptés par les comités techniques sont soumis aux comités membres pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des comités membres votants.

La Norme internationale ISO 9735-7 a été élaborée par la Division du commerce de la Commission Économique pour l'Europe des Nations Unies (en tant qu'EDIFACT/ONU) et a été adoptée, selon une procédure spéciale par «voie express», par le comité technique ISO/TC 154, *Documents et éléments de données dans l'administration, le commerce et l'industrie*.

Alors que la présente partie remplace les publications antérieures et qu'un numéro de version «4» doit être attribué à l'élément de données obligatoire 0002 (numéro de version de syntaxe) du segment UNB (en-tête de l'échange), les échanges continuant à utiliser la syntaxe définie dans les versions publiées antérieurement doivent reprendre les numéros suivants de version de syntaxe, afin de se différencier tant les uns des autres que de la présente partie:

ISO 9735:1988 — *Numéro de version de syntaxe: 1*

ISO 9735:1988 (modifiée et réimprimée en 1990) — *Numéro de version de syntaxe: 2*

ISO 9735:1988 (modifiée et réimprimée en 1990) plus Amendement 1:1992 — *Numéro de version de syntaxe: 3*

L'ISO 9735 comprend les parties suivantes, présentées sous le titre général *Échange de données informatisé pour l'administration, le commerce et le transport (EDIFACT) — Règles de syntaxe au niveau de l'application (numéro de version de syntaxe: 4)*:

— *Partie 1: Règles de syntaxe communes à l'ensemble des parties, accompagnées des répertoires de service syntaxiques associés à chacune d'elles*

— *Partie 2: Règles de syntaxe spécifiques à l'EDI par lots*

— *Partie 3: Règles de syntaxe spécifiques à l'EDI interactif*

— *Partie 4: Message Compte rendu syntaxique et de service pour l'EDI par lots (type de message CONTRL)*

— *Partie 5: Règles de sécurité pour l'EDI par lots (authentification, intégrité et non-répudiation de l'origine)*

— *Partie 6: Message sécurisé Authentification et accusé de réception (type de message AUTACK)*

— *Partie 7: Règles de sécurité pour le lot EDI (confidentialité)*

— *Partie 8: Données associées en EDI*

— *Partie 9: Message Gestion de clés et de certificats de sécurité (type de message KEYMAN)*

— *Partie 10: Règles de sécurité pour l'EDI interactif*

D'autres parties pourront être ajoutées ultérieurement.

L'annexe A constitue un élément normatif de la présente partie de l'ISO 9735. Les annexes B, C et D ne sont données qu'à titre d'information.

Introduction

La présente partie de l'ISO 9735 comprend les règles qui se situent au niveau de l'application pour la structuration des données associées à l'échange de messages électroniques dans un environnement ouvert, fondées sur les prescriptions du traitement ou par lots, ou interactif. Ces règles ont été adoptées par la Commission Économique pour l'Europe des Nations Unies (CEE/ONU) comme règles de syntaxe pour l'échange de données informatisé pour l'administration, le commerce et le transport (EDIFACT). Elles font partie du Répertoire d'Échange de données commerciales des Nations Unies (UNTDID) qui comporte également les Directives pour la conception de messages, tant par transmission par lots qu'en mode interactif.

La présente partie de l'ISO 9735 peut être utilisée dans toute application, mais seuls les messages qui les prennent en compte peuvent se prévaloir d'être des messages EDIFACT s'ils respectent les autres directives, règles et répertoires contenus dans le Répertoire d'échange de données commerciales des Nations Unies. Pour être EDIFACT/ONU, les messages doivent être conformes aux règles de conception des messages destinés à une utilisation par lots ou en mode interactif. Les règles sont maintenues dans le Répertoire d'échange des données commerciales.

Les spécifications des communications et les protocoles n'entrent pas dans le cadre de la présente partie de l'ISO 9735.

La présente partie est nouvelle, elle a été ajoutée à l'ISO 9735. Elle offre la possibilité d'appliquer la confidentialité à une structure EDIFACT, à savoir un message, paquet, groupe ou échange.

Échange de données informatisé pour l'administration, le commerce et le transport (EDIFACT) — Règles de syntaxe au niveau de l'application (numéro de version de syntaxe: 4) —

Partie 7:
Règles de sécurité pour le lot EDI (confidentialité)

1 Domaine d'application

La présente partie de l'ISO 9735 est destinée à la sécurité EDIFACT par lots et traite de la sécurité sur le plan de la confidentialité aux niveaux du message/paquet, du groupe et de l'échange conformément aux mécanismes de sécurité reconnus.

2 Conformité

La conformité à une norme signifie que la totalité de ses prescriptions, y compris tous ses aspects, sont pris en compte. Si tel n'est pas le cas, toute demande de conformité doit comporter une déclaration identifiant chacun des aspects qui en fait l'objet.

Les données échangées sont en conformité si la structure et la représentation des données respectent les règles de syntaxe définies dans la présente partie de l'ISO 9735.

Les dispositifs qui s'appuient sur la présente partie de l'ISO 9735 sont en conformité s'ils sont en mesure de créer et/ou d'interpréter les données structurées et représentées conformément à la présente norme.

La conformité à la présente partie doit prendre en compte la conformité à l'ISO 9735-1, l'ISO 9735-2 et l'ISO 9735-5.

Une fois identifiées dans la présente partie de l'ISO 9735, les dispositions définies dans les normes associées devront faire partie intégrante des critères de conformité.

3 Références normatives

Les documents normatifs suivants contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions valables pour la présente partie de l'ISO 9735. Pour les références datées, les amendements ultérieurs ou les révisions de ces publications ne s'appliquent pas. Toutefois, les parties prenantes aux accords fondés sur la présente partie de l'ISO 9735 sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des documents normatifs indiqués ci-après. Pour les références non datées, la dernière édition du document normatif en référence s'applique. Les membres de l'ISO et de la CEI possèdent le registre des Normes internationales en vigueur.

ISO 9735-1:1998, *Échange de données informatisé pour l'administration, le commerce et le transport (EDIFACT) — Règles de syntaxe au niveau de l'application (numéro de version de syntaxe: 4) — Partie 1: Règles de syntaxe communes à l'ensemble des parties, accompagnées des répertoires de services syntaxiques associés à chacune d'elles.*

ISO 9735-2:1998, *Échange de données informatisé pour l'administration, le commerce et le transport (EDIFACT) — Règles de syntaxe au niveau de l'application (numéro de version de syntaxe: 4) — Partie 2: Règles de syntaxe spécifiques à l'EDI par lots.*

ISO 9735-5:1999, *Échange de données informatisé pour l'administration, le commerce et le transport (EDIFACT) — Règles de syntaxe au niveau de l'application (numéro de version de syntaxe: 4) — Partie 5: Règles de sécurité pour l'EDI par lots (authentification, intégrité et non-répudiation de l'origine).*

ISO/CEI 10181-5:1996, *Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — Cadre de sécurité pour les systèmes ouverts: Cadre de confidentialité.*

4 Définitions

Pour les besoins de la présente partie de l'ISO 9735, les définitions données dans l'ISO 9735-1:1998, annexe A, s'appliquent.

5 Règles de confidentialité pour l'EDI par lots

5.1 Confidentialité EDIFACT

Les risques pouvant menacer la transmission des données EDIFACT et les services de sécurité qui en traitent sont décrits dans l'ISO 9735-5:1999, annexes A et B.

Cette section décrit la solution permettant d'assurer le service de sécurité appliqué à la confidentialité des structures EDIFACT.

La confidentialité d'une structure EDIFACT (message, paquet, groupe ou échange) doit être assurée par le chiffrement respectif du corps d'un message, d'un objet, de messages/paquets ou de messages/paquets/groupes, ainsi que par l'utilisation de tout autre groupe de segments d'en-tête et de fin de sécurité s'appuyant sur un algorithme cryptographique approprié. Ces données chiffrées peuvent être filtrées pour être utilisées par des réseaux de télécommunication aux capacités limitées.

5.1.1 Confidentialité pour l'EDI par lots

5.1.1.1 Confidentialité d'un échange

La Figure 1 représente la structure d'un seul échange sécurisé par la confidentialité. La chaîne de caractères de service (UNA), le segment d'en-tête d'échange (UNB) et le segment de fin d'échange (UNZ) ne sont pas affectés par le chiffrement.

Si la compression est appliquée, elle doit l'être avant le chiffrement.

Le chiffrement, la compression, l'algorithme du filtre et les paramètres sont définis dans le groupe de segments d'en-tête de sécurité.

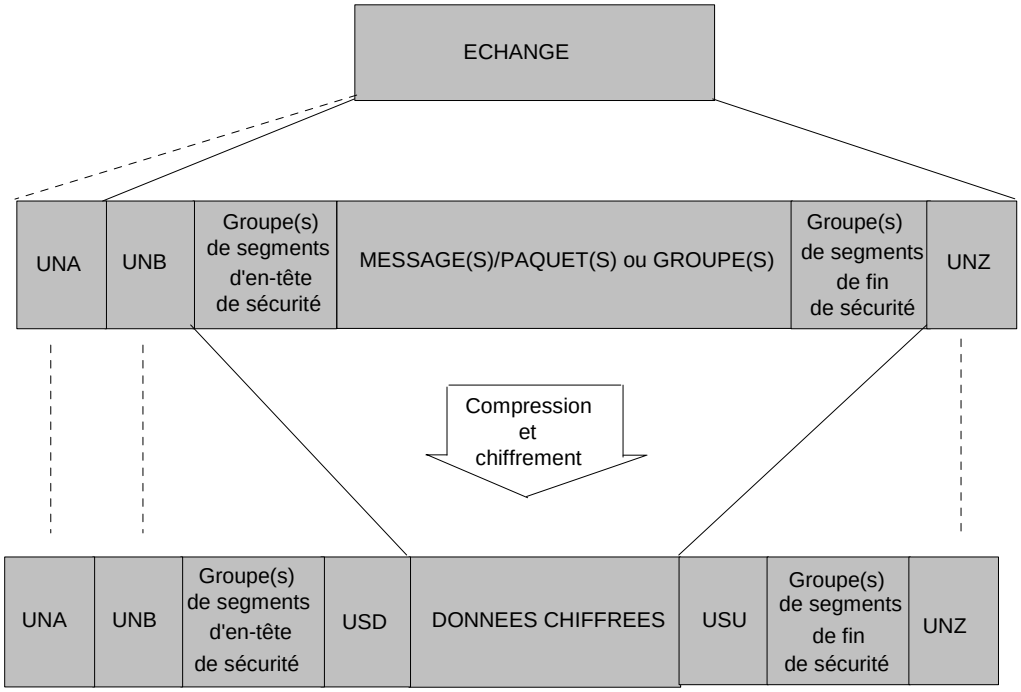

Figure 1 — Structure d'un échange dont le contenu [message(s)/paquet(s) ou groupe(s)] a été chiffré (schéma simplifié)

5.1.1.2 Confidentialité d'un groupe

La Figure 2 représente la structure d'un échange contenant un groupe chiffré qui a également été sécurisé pour d'autres applications de sécurité. Le segment d'en-tête de groupe (UNG) et le segment de fin de groupe (UNE) ne sont pas affectés par le chiffrement.

Si la compression est appliquée, elle doit l'être avant le chiffrement.

Le chiffrement, la compression, l'algorithme du filtre et les paramètres sont définis dans le groupe de segments d'en-tête de sécurité.

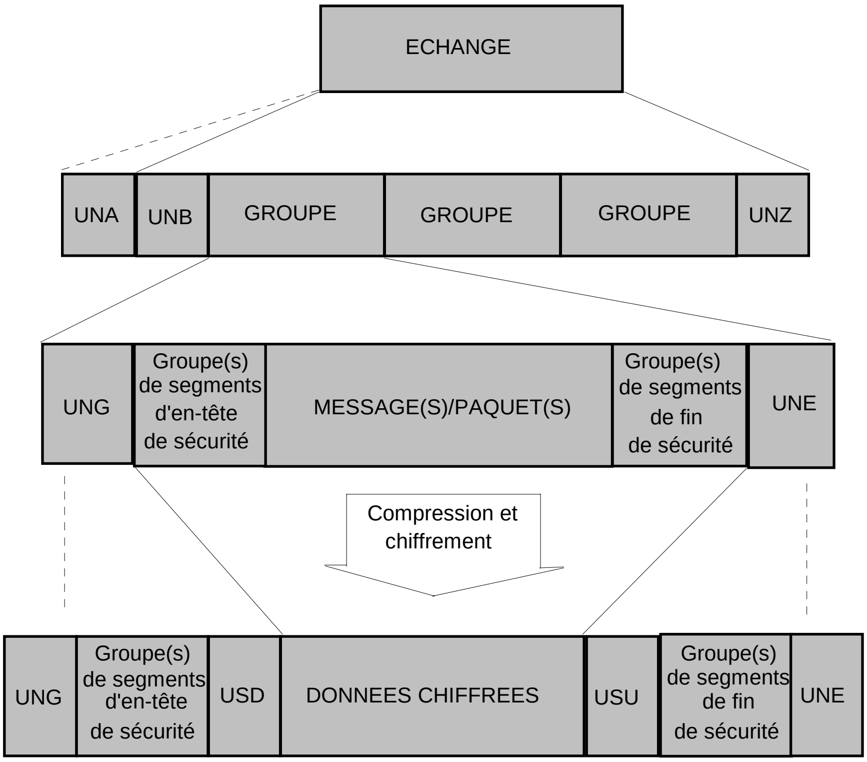

Figure 2 — Structure d'un échange contenant un seul groupe dont le contenu (corps du groupe et groupes associés des segments d'en-tête et de fin de sécurité) a été chiffré (schéma simplifié)

5.1.1.3 Confidentialité d'un message

La Figure 3 représente la structure d'un échange contenant un seul message chiffré qui a également été sécurisé pour une autre application de sécurité. Le segment d'en-tête de message (UNH) et le segment de fin de message (UNT) ne sont pas affectés par le chiffrement.

Si la compression est appliquée, elle doit l'être avant le chiffrement.

Le chiffrement, la compression, l'algorithme du filtre et les paramètres sont définis dans le groupe de segments d'en-tête de sécurité.

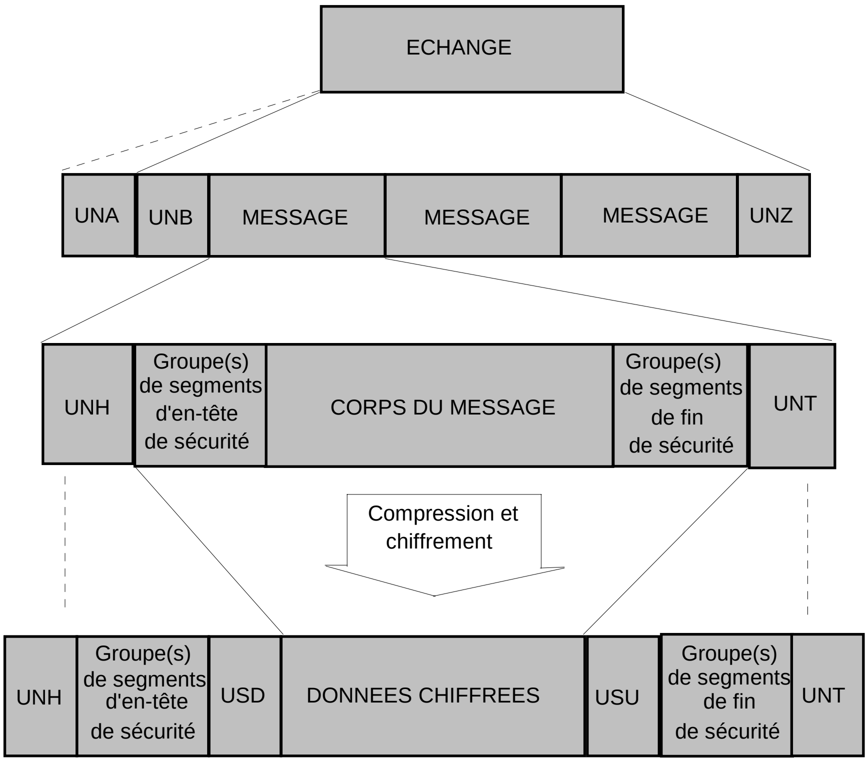

Figure 3 — Structure d'un échange contenant un seul message dont le contenu (corps du message et groupes associés des segments d'en-tête et de fin de sécurité) a été chiffré (schéma simplifié)

5.1.1.4 Confidentialité d'un paquet

La Figure 4 représente la structure d'un échange contenant un seul paquet chiffré qui a également été sécurisé pour une autre application de sécurité. Le segment d'en-tête d'objet (UNO) et le segment de fin d'objet (UNP) ne sont pas affectés par le chiffrement

Si la compression est appliquée, elle doit l'être avant le chiffrement.

Le chiffrement, la compression, l'algorithme du filtre et les paramètres sont définis dans le groupe de segments d'en-tête de sécurité.

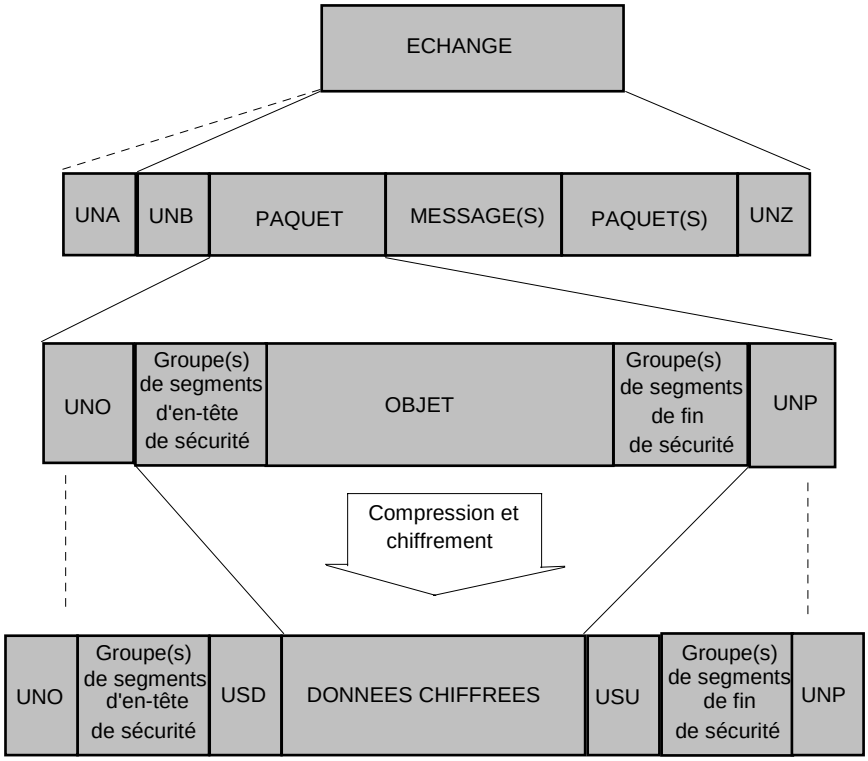

Figure 4 —Structure d'un échange contenant un seul paquet dont le contenu (objet et groupes associés des segments d'en-tête et de fin de sécurité) a été chiffré (schéma simplifié)

5.1.2 Structure des segments d'en-tête et de fin de sécurité pour le chiffrement des données

ETIQUETTE	Nom	S	R
	Groupe de segments 1	C	99
USH	En-tête de sécurité	M	1
USA	Algorithme de sécurité	C	3
	Groupe de segments 2	C	2
USC	Certificat	M	1
USA	Algorithme de sécurité	C	3
USR	Résultat de la sécurité	C	1
USD	En-tête de chiffrement des données	M	1
	Données chiffrées		
USU	Fin de chiffrement des données	M	1
	Groupe de segments n	C	99
UST	Fin de sécurité	M	1
USR	Résultat de la sécurité	C	1

Figure 5 — Table de segments des groupes de segments d'en-tête et de fin de sécurité

NOTE Les segments USH, USA, USC, USR et UST sont définis dans l'ISO 9735-5. Ils ne sont pas décrits plus loin dans la présente partie.