NORME INTERNATIONALE

ISO 9735-5

Première édition
1999-04-01

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 5:

Règles de sécurité pour l'EDI par lots (authentification, intégrité et non-répudiation de l'origine)

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

Part 5: Security rules for batch EDI (authenticity, integrity and non-repudiation of origin)

Numéro de référence
ISO 9735-5:1999(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 9735-5 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 la 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.

Les annexes A et B constituent des éléments normatifs de la présente partie de l'ISO 9735. Les annexes C à I 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.

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 de sécuriser des structures EDIFACT par lots, c'est à dire des messages, des paquets, des groupes ou un échange.

Échange de données informatisé pour l'administration, le commerce et l'industrie (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)

1 Domaine d'application

La présente partie de l'ISO 9735 définit les règles de syntaxe régissant la sécurité EDIFACT. Elle décrit une méthode traitant de la sécurité au niveau d'un message/paquet, d'un groupe et d'un échange permettant d'assurer l'authenticité, l'intégrité et la non-répudiation de l'origine, conformément aux mécanismes reconnus de sécurité.

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 partie de l'ISO 9735.

La conformité à la présente partie l'ISO 9735 doit prendre en compte la conformité aux Parties 1, 2 et 8 de l'ISO 9735.

Une fois identifiées dans la présente partie de l'ISO 9735, les dispositions définies dans les normes associées doivent 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 7498-2:1989, *Systèmes de traitement de l'information — Interconnexion de systèmes ouverts — Modèle de référence de base — Partie 2: Architecture de sécurité.*

ISO/CEI 9594-8:1995, *Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — L'Annuaire: Cadre d'authentification.*

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 service 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 9735-6:1999, *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 6: Message sécurisé Authentification et accusé de réception (type de message AUTACK).*

ISO 9735-7:—[1)], *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)*.

ISO 9735-8:1998, *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 8: Données associées en EDI.*

ISO/CEI 10181-2:1996, *Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — Cadres de sécurité pour les systèmes ouverts: Cadre d'authentification.*

ISO/CEI 10181-4:1997, *Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — Cadres de sécurité pour les systèmes ouverts: Cadre de non-répudiation.*

ISO/CEI 10181-6:1996, *Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — Cadres de sécurité pour les systèmes ouverts: Cadre d'intégrité.*

4 Définitions

Pour les besoins de la présente partie de l'ISO 9735, les définitions données dans l'annexe A de l'ISO 9738-1:1998 s'appliquent.

5 Règles d'utilisation des groupes de segments d'en-tête et de fin de sécurité pour l'EDI par lots

5.1 Sécurité au niveau d'un message/paquet - sécurité intégrée à un message/paquet

Les risques pouvant menacer la sécurité de la transmission d'un message/paquet et les services de sécurité qui en traitent sont décrits dans les annexes C et D.

Cette section décrit la structure de la sécurité au niveau d'un message/paquet EDIFACT.

Les services de sécurité traités dans la présente partie de l'ISO 9735 doivent être assurés par l'inclusion de groupes de segments d'en-tête et de fin de sécurité après le segment UNH et avant le segment UNT de façon à s'appliquer à tout message existant, ou après le segment UNO et avant le segment UNP, pour tout paquet existant.

1) À publier.

5.1.1 Groupes de segments d'en-tête et de fin de sécurité

La Figure 1 décrit un échange illustrant l'application de la sécurité au niveau d'un message.

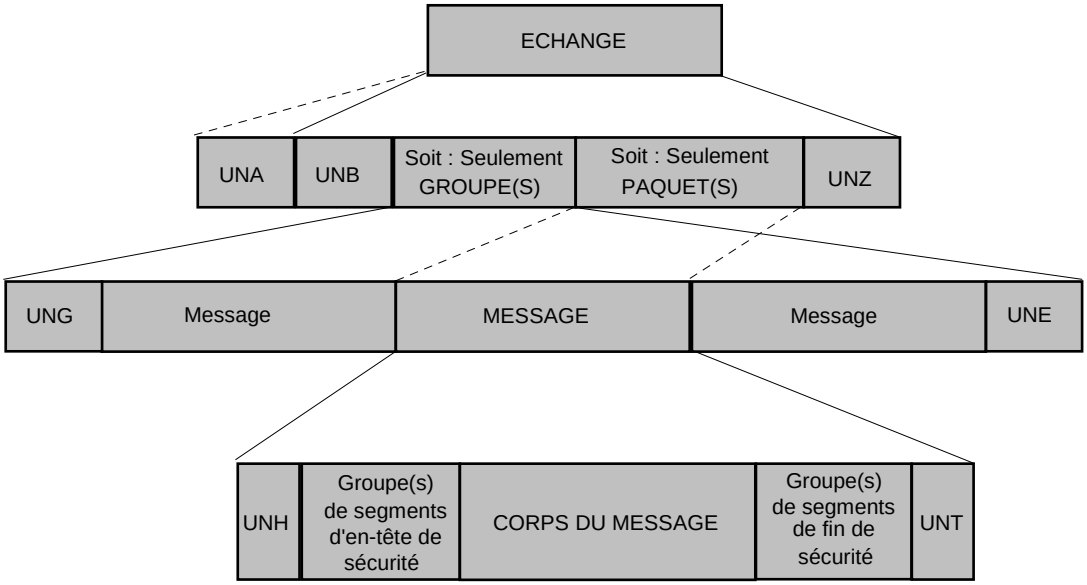

Figure 1 — Échange illustrant l'application de la sécurité au niveau d'un message (schéma simplifié)

La Figure 2 décrit un échange illustrant l'application de la sécurité au niveau d'un paquet.

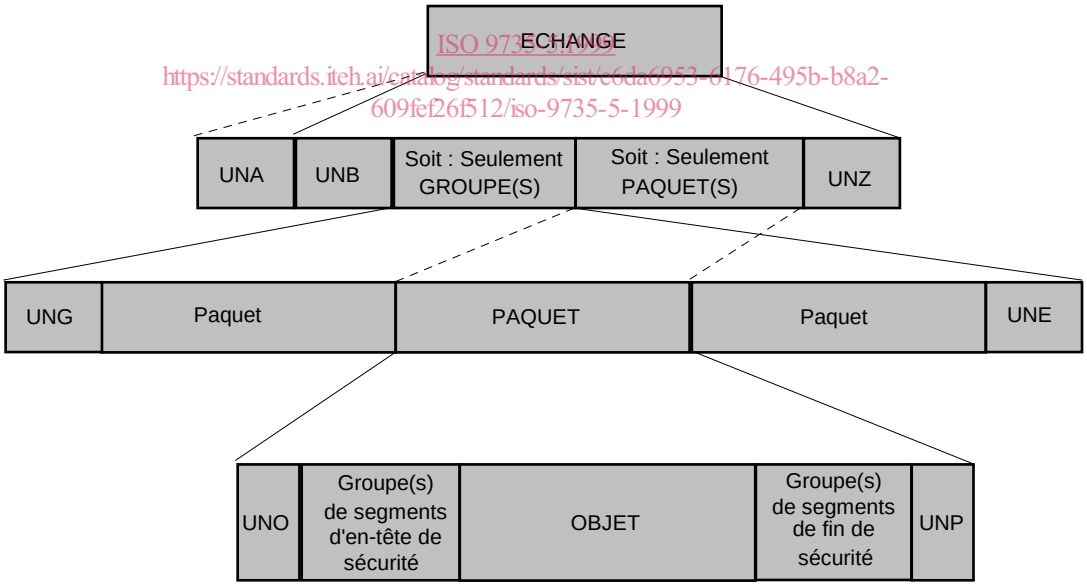

Figure 2 — Échange illustrant l'application de la sécurité au niveau d'un paquet (schéma simplifié)

5.1.2 Structure de groupes de segments d'en-tête et de fin de sécurité

Tableau 1 — Table des segments des groupes de segments d'en-tête et de fin de sécurité (sécurité au niveau du message)

Etiquette	Nom	S	R	
UNH	En-tête de message	M	1	
-----	Groupe de segments 1----------	C	99	--------+
USH	En-tête de sécurité	M	1	I
USA	Algorithme de sécurité	C	3	I
-----	Groupe de segments 2----------	C	2	----+ I
USC	Certificat	M	1	I I
USA	Algorithme de sécurité	C	3	I I
USR	Résultat de sécurité	C	1	--------+
	Corps du message			
-----	Groupe de segments n----------	C	99	----+
UST	Fin de sécurité	M	1	I
USR	Résultat de la sécurité	C	1	----+
UNT	Fin de message	M	1	

Tableau 2 — Table des segments des groupes de segments d'en-tête et de fin de sécurité (sécurité au niveau du paquet)

Etiquette	Nom	S	R	
UNO	En-tête d'objet	M	1	
-----	Groupe de segments 1----------	C	99	--------+
USH	En-tête de sécurité	M	1	I
USA	Algorithme de sécurité	C	3	I
-----	Groupe de segments 2----------	C	2	----+ I
USC	Certificat	M	1	I I
USA	Algorithme de sécurité	C	3	I I
USR	Résultat de la sécurité	C	1	--------+
	Objet			
-----	Groupe de segments n----------	C	99	----+
UST	Fin de sécurité	M	1	I
USR	Résultat de la sécurité	C	1	----+
UNP	Fin d'objet	M	1	

NOTE L'en-tête UNH du message, la fin UNT du message, l'en-tête UNO d'objet et la fin UNP d'objet sont décrits dans la Partie 1 de l'ISO 9735. Ils ne sont pas décrits plus loin dans la présente partie.

Toutes les spécifications des segments et des éléments de données peuvent être consultées dans l'annexe B qui contient les répertoires correspondants.

5.1.3 Précisions sur les segments de données

Groupe de segments 1: USH-USA-SG2 (groupe d'en-tête de sécurité)

Groupe de segments identifiant le service et les mécanismes de sécurité qui s'appliquent et contenant les données nécessaires à l'exécution des calculs de validation.

Il peut y avoir plusieurs groupes de segments d'en-tête de sécurité dans le même message/paquet, si différents services de sécurité s'appliquent au message/paquet (par exemple, intégrité et non-répudiation de l'origine) ou si le même service de sécurité s'applique à plusieurs intervenants.

USH, En-tête de sécurité

Segment définissant un service de sécurité s'appliquant au message/paquet dans lequel ce segment est intégré.

Les intervenants impliqués dans le service de sécurité (initiateur des éléments de sécurité et destinataire des éléments de sécurité) peuvent être identifiés dans ce segment, à moins qu'ils soient identifiés sans ambiguïté par des certificats (segment USC) lorsque des algorithmes asymétriques sont utilisés.

L'élément de données composite (S500) «Précisions concernant les informations détaillées sur l'identification» doit être utilisé dans le segment USH, dans les cas suivants :

— si des algorithmes symétriques sont utilisés, ou

— si des algorithmes asymétriques sont utilisés et que deux certificats sont présents, afin d'opérer la distinction entre les certificats de l'initiateur et du destinataire.

Dans ce dernier cas, «l'identification de l'intervenant» contenue dans l'élément de données composite S500 (l'un ou l'autre des éléments de données S500/0511, S500/0513, S500/0515, S500/0586) doit être la même que l'identification de l'intervenant, qualifié de «propriétaire de certificat», contenue dans l'une des données de S500 présente dans le segment USC du groupe de segments 2 et l'élément de données S500/0577 doit identifier la fonction (initiateur ou destinataire) de l'intervenant impliqué.

L'élément de données «Nom de la clé» contenu dans l'élément de données composite, «Informations détaillées sur l'identification de l'intervenant» (S500/0538), peut servir à établir la relation des clés entre l'émetteur et le récepteur.

Cette relation peut également être établie en utilisant l'élément de données «Identification de la clé» contenu dans l'élément de données composite «Paramètre de l'algorithme» (S503/0554) contenu dans le segment USA du groupe de segments 1.

L'élément de données composite S500/0538 contenu dans le segment USH peut être utilisé s'il n'est pas nécessaire de véhiculer un segment USA dans le groupe de segments 1 (les mécanismes cryptographiques ayant été convenus au préalable entre les partenaires).

Néanmoins, il est vivement recommandé d'utiliser soit S500/0538 du segment USH, ou S503/0554 avec le qualifiant approprié du segment USA, mais non les deux, au sein du même groupe d'en-tête de sécurité.

Le segment USH peut indiquer la fonction du filtre utilisé pour les champs binaires du segment USA au sein du groupe de segments 1 et du segment USR du groupe correspondant de fin de sécurité.

Le segment USH peut comprendre un numéro de séquence de sécurité pour indiquer l'intégrité d'une séquence et la date de création des éléments de sécurité.

USA, Algorithme de sécurité

Segment identifiant un algorithme de sécurité, l'utilisation technique qui en est faite et contenant les paramètres techniques requis. Il s'agira de l'algorithme s'appliquant directement au message/paquet. Cet algorithme peut être soit symétrique, soit une fonction de hachage, soit un algorithme de compression. Il indique la fonction à utiliser par exemple, pour une signature numérique. Il ne doit pas être fait référence aux algorithmes asymétriques directement dans ce segment USA contenu dans le groupe de segments 1 car ces algorithmes ne peuvent apparaître que dans le groupe de segments 2, déclenché par un segment USC.

Trois occurrences du segment USA sont autorisées. Une occurrence doit être utilisée pour l'algorithme ou la fonction de hachage nécessaire à la fourniture du service de sécurité défini dans le segment USH segment. Les deux autres occurrences sont décrites dans la Partie 7 de l'ISO 9735.

Un mécanisme de remplissage peut être indiqué aux endroits appropriés.

Groupe de segments 2: USC-USA-USR (certificat)

Groupe de segments contenant les données nécessaires à la validation des méthodes de sécurité s'appliquant au message/paquet, lorsque des algorithmes asymétriques sont utilisés. Le groupe de segments du certificat doit être utilisé lorsque des algorithmes asymétriques sont utilisés pour identifier la paire de clés asymétriques utilisée, même si des certificats ne sont pas utilisés.

Soit l'ensemble du groupe de segments (comprenant le segment USR), soit les seuls éléments de données nécessaires à l'identification non ambiguë de la paire de clés asymétriques utilisée, doivent être présents dans le segment USC. La présence d'un certificat complet peut être évitée si le certificat a déjà été échangé entre les deux partenaires ou s'il peut être extrait d'une base de données.

S'il est décidé de faire référence à un certificat non EDIFACT (tel qu'à un X.509), la syntaxe et la version de ce certificat doivent être identifiés dans l'élément de données 0545 du segment USC. Ces certificats peuvent être véhiculés dans un paquet EDIFACT.

Deux occurrences de ce groupe de segments sont autorisées, l'une correspondant au certificat de l'émetteur du message/paquet (qui servira au récepteur du message/paquet à vérifier la signature de l'émetteur), l'autre correspondant au certificat du récepteur de ce message/paquet (auquel il n'est fait référence que par la référence du certificat) au cas où la clé publique du récepteur est utilisée par l'émetteur pour des raisons de confidentialité de clés symétriques.

SI les deux sont présentes au sein d'un groupe de segments d'en-tête de sécurité, l'élément de données composite «Informations détaillées sur l'identification de la sécurité» (S500) ainsi que l'élément de données «Référence du certificat» (0536) permettront de les différencier.

Ce groupe de segments doit être omis si aucun algorithme asymétrique n'est utilisé.

USC, Certificat

Segment contenant les justificatifs d'identité du propriétaire du certificat et identifiant l'autorité de certification qui a généré le certificat. L'élément de données «Fonction du filtre, en code», (0505) doit identifier la fonction du filtre utilisé pour les champs binaires des segments USA et du segment USR au sein du groupe de segments 2.

Le certificat USC peut contenir deux occurrences de l'élément de données S500: l'une pour le propriétaire du certificat (identifiant l'intervenant qui signe avec la clé privée associée à la clé publique contenue dans ce certificat), l'autre pour l'émetteur du certificat (autorité de certification ou «CA»).

USA, Algorithme de sécurité

Segment identifiant un algorithme de sécurité, l'utilisation technique qui en est faite et contenant les paramètres techniques requis. Les trois occurrences différentes de ce segment USA dans le groupe de segments 2 identifient

1 l'algorithme utilisé pour l'émetteur pour calculer la valeur de hachage du certificat (fonction de hachage);

2 l'algorithme utilisé par l'émetteur du certificat pour produire le certificat (c'est-à-dire le résultat de la fonction de hachage calculé à partir du contenu du certificat) (algorithme asymétrique);

3a soit l'algorithme utilisé par l'émetteur pour signer le message/paquet (c'est-à-dire, pour signer le résultat de la fonction de hachage décrite dans le segment USH, calculé à partir du contenu du message/paquet) (algorithme asymétrique);

3b soit l'algorithme asymétrique du récepteur, utilisé par l'émetteur pour chiffrer la clé requise, par un algorithme symétrique appliqué au contenu du message/paquet et auquel fait référence le groupe de segments 1 déclenché par le segment USH) (algorithme asymétrique).

L'indication du mécanisme de remplissage peut être utilisée.

USR, Résultat de sécurité

Segment contenant le résultat des fonctions de sécurité appliquées au certificat par l'autorité de certification. Ce résultat doit être constitué par la signature du certificat calculée par l'autorité de certification en signant le résultat de hachage calculé à partir des données du justificatif d'identité.

Pour le certificat, le calcul de la signature commence au premier caractère du segment USC (à savoir le «U») et se termine au dernier caractère du dernier segment USA (qui comprend le séparateur qui suit ce segment USA).

Groupe de segments n: UST-USR (groupe de fin de sécurité)

Groupe de segments contenant un lien avec le groupe de segments d'en-tête de sécurité et le résultat des fonctions de sécurité appliquées au message/paquet.

UST, Fin de sécurité

Segment établissant un lien entre le groupe de segments d'en-tête de sécurité et de fin de sécurité et indiquant le nombre de segments de sécurité contenu dans ces groupes.

USR, Résultat de sécurité

Segment contenant le résultat des fonctions de sécurité appliquées au message/paquet comme précisé dans le groupe d'en-tête de sécurité subordonné. En fonction des mécanismes de sécurité définis dans le groupe d'en-tête de sécurité subordonné, ce résultat doit être, soit

— directement calculé à partir du message/paquet par l'algorithme défini dans le segment USA au sein du groupe de segments 1 du groupe d'en-tête de sécurité ou

— calculé en signant, avec un algorithme asymétrique défini dans le segment USA au sein du groupe de segments 2 du groupe de segments d'en-tête de sécurité, un résultat de hachage calculé à partir du message/paquet par l'algorithme défini dans le segment USA au sein du groupe de segments 1 du groupe de segments d'en-tête de sécurité.

5.1.4 Domaine d'application de la sécurité

La sécurité peut s'appliquer dans deux domaines :

1. Le calcul de chacune des valeurs d'intégrité et d'authentification et des signatures numériques commence par, et comprend, le groupe de segments d'en-tête de sécurité courant et le corps du message ou l'objet, lui-même. Dans ce cas, aucun autre groupe de segments d'en-tête ou de fin de sécurité ne doit entrer dans ce domaine.

   Le décompte du groupe de segments d'en-tête de sécurité doit être effectué à partir du premier caractère, à savoir «U», jusqu'au séparateur terminant le groupe de segments d'en-tête de sécurité, les deux compris et le corps du message, ou l'objet, à partir du premier caractère suivant le séparateur terminant le dernier groupe de segments d'en-tête de sécurité jusqu'au séparateur précédant le premier caractère du premier groupe de segments de fin de sécurité, les deux compris.

   Ainsi l'ordre dans lequel les services de sécurité intégrés de cette façon sont exécutés, n'est pas imposé. Ils sont totalement indépendants les uns des autres.

   La Figure 3 illustre ce cas (le domaine d'application du service de sécurité défini dans l'en-tête 2 est représenté par des cases en grisé).

UNH/ *UNO*	Groupe de segments d'en-tête de sécurité 3	Groupe de segments d'en-tête de sécurité 2	Groupe de segments d'en-tête de sécurité 1	CORPS DU MESSAGE/ *OBJET*	Groupe de segments de fin de sécurité 1	Groupe de segments de fin de sécurité 2	Groupe de segments de fin de sécurité 3	UNT/ *UNP*

Figure 3 — Domaine d'application: groupe de segments d'en-tête de sécurité et corps du message/objet seulement (schéma simplifié)

2. Le calcul commence par, et comprend, le groupe courant de segments d'en-tête de sécurité jusqu'au groupe de segments de fin de sécurité associé. Dans ce cas, le groupe courant de segments d'en-tête de sécurité, le corps du message, ou l'objet, et tous les autres groupes de segments d'en-tête de sécurité et de fin de sécurité imbriqués, doivent entrer dans ce domaine.

   Le domaine d'application doit comprendre tous les caractères à partir du premier caractère, à savoir «U» du groupe courant de segments d'en-tête de sécurité, jusqu'au séparateur précédant le premier caractère du groupe de segments de fin de sécurité associé, les deux compris.

   La Figure 4 illustre ce cas (le domaine d'application du service de sécurité défini dans l'en-tête de sécurité 2 est représenté dans les cases en grisé).

UNH/ *UNO*	Groupe de segments d'en-tête de sécurité 3	Groupe de segments d'en-tête de sécurité 2	Groupe de segments d'en-tête de sécurité 1	CORPS DU MESSAGE/ *OBJET*	Groupe de segments de fin de sécurité 1	Groupe de segments de fin de sécurité 2	Groupe de segments de fin de sécurité 3	UNT/ *UNP*

Figure 4 — Domaine d'application: du groupe de segments d'en-tête de sécurité au groupe de segments de fin de sécurité (schéma simplifié)

Pour chaque service de sécurité ajouté, l'une des deux démarches peut être retenue.

Dans les deux cas, la relation entre le groupe de segments d'en-tête de sécurité et le groupe de segments de fin de sécurité associé doit être fournie par les éléments de données «Numéro de la référence de la sécurité» des segments USH et UST.

5.2 Principes d'utilisation

5.2.1 Choix du service

Le groupe de segments d'en-tête de sécurité peut comporter les informations générales qui suivent :

— service de sécurité appliqué

— identification des intervenants impliqués

— mécanisme de sécurité utilisé

— valeur «Unique» (numéro de séquence et/ou horodatage)

— non-répudiation de demande de réception

Si plus d'un service de sécurité est requis pour la même structure EDIFACT, le groupe de segments d'en-tête de sécurité peut alors être présent plusieurs fois. Ce sera le cas lorsque plusieurs couples d'intervenants seront impliqués. Cependant si plusieurs services sont requis entre le même couple d'intervenants, ils peuvent être incorporés dans une seule paire de groupes de segments d'en-tête et de fin de sécurité, puisque certains services en comportent implicitement d'autres.

5.2.2 Authenticité

Si l'authentification de l'origine d'une structure EDIFACT est requise, elle doit être fournie conformément aux principes définis dans l'ISO 10181-2, par l'utilisation d'une paire appropriée de groupes de segments d'en-tête et de fin de sécurité.

Le service de sécurité de l'authentification de l'origine doit être défini dans le segment USH et l'algorithme, être identifié dans le segment USA du groupe de segments 1. Cet algorithme doit être symétrique.

L'intervenant jouant le rôle d'initiateur de sécurité doit calculer une valeur de l'authenticité qui doit être véhiculée dans le segment USR du groupe de segments de fin de sécurité. L'intervenant jouant le rôle de destinataire doit vérifier la valeur de l'authenticité.

Ce service pouvant comporter un service d'intégrité peut être obtenu en tant que sous-produit de service de non-répudiation de l'origine.

Si la mise en œuvre appropriée de ce service «d'authentification de l'origine», fondée sur un matériel infalsifiable ou sur des tiers certificateurs, est assurée, elle peut être considérée comme une instance de service de «non-répudiation de l'origine». Cette pratique doit être définie dans l'accord d'échange.

5.2.3 Intégrité

Si l'intégrité du contenu d'une structure EDIFACT est requise, elle doit être fournie conformément aux principes définis dans l'ISO 10181-6, par l'utilisation d'une paire appropriée de groupes de segments d'en-tête et de fin de sécurité.

Le service sécurisé de l'intégrité doit être défini dans le segment USH et l'algorithme, identifié dans le segment USA du groupe de segments 1. Il doit s'agir d'une fonction de hachage ou d'un algorithme symétrique.

L'intervenant jouant le rôle d'initiateur de la sécurité doit calculer une valeur d'intégrité qui doit être véhiculée dans le segment USR du groupe de segments de fin de sécurité. L'intervenant jouant le rôle de destinataire de la sécurité doit vérifier la valeur de l'intégrité.

Ce service peut être obtenu en tant que sous-produit du service de l'authentification de l'origine ou de non-répudiation de l'origine.

Si l'intégrité d'une séquence est requise, le groupe de segments d'en-tête doit contenir, soit, un numéro de séquence de sécurité, soit, un horodatage de sécurité, ou bien les deux, et il conviendra d'utiliser les services d'intégrité du contenu ou d'authentification de l'origine ou de non-répudiation de l'origine.

5.2.4 Non-répudiation de l'origine

Si la non-répudiation de l'origine d'une structure EDIFACT est requise, elle doit être fournie conformément aux principes définis dans l'ISO 10181-4, par l'utilisation d'une paire appropriée de groupes de segments d'en-tête et de fin de sécurité.

Le service sécurisé de non-répudiation de l'origine doit être défini dans le segment USH et l'algorithme de hachage, identifié dans le segment USA du groupe de segments 1 et l'algorithme asymétrique utilisé pour la signature, dans les segments USA du groupe de segments 2, si des certificats sont utilisés.

Si le certificat n'est pas véhiculé dans le message/paquet, l'algorithme asymétrique doit être implicitement connu de l'intervenant récepteur. Dans ce cas, l'algorithme asymétrique doit être défini dans l'accord d'échange.

L'acteur jouant le rôle d'initiateur de la sécurité doit calculer une valeur numérique qui doit être véhiculée dans le segment USR du groupe de segments de fin de sécurité. L'acteur jouant le rôle de destinataire doit vérifier la valeur de la signature numérique.

Ce service comprend également les services d'intégrité et d'authentification de l'origine.