NORME INTERNATIONALE

ISO 9735-6

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 6:

Message sécurisé Authentification et accusé de réception (type de message AUTACK)

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

Part 6: Secure authentication and acknowledgement message (message type-AUTACK)

Numéro de référence
ISO 9735-6:1999(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 9735-6 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.

L'annexe A constitue un élément normatif de la présente partie de l'ISO 9735. Les annexes B à E 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 est nouvelle. Elle a été ajoutée à l'ISO 9735. Elle offre la possibilité de sécuriser des structures EDIFACT, c'est-à-dire des messages, des paquets, des groupes ou des échanges au moyen d'un message sécurisé d'authentification et d'accusé de réception.

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)

1 Domaine d'application

La présente partie de l'ISO 9735 est destinée à la sécurité EDIFACT et définit le message Authentification et accusé de réception sécurisé AUTACK.

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 de l'ISO 9735 doit prendre en compte la conformité aux Parties 1, 2 et 5 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 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 9735-5:1999, *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).*

4 Définitions

Pour les besoins de la présente partie de l'ISO 9735, les définitions données dans l'ISO 9735-1:1998, annexe A, et dans l'ISO 9735-5:1999, annexe A, s'appliquent.

5 Règles d'utilisation du message sécurisé Authentification et accusé de réception

5.1 Définition fonctionnelle

AUTACK est un message authentifiant des échanges, groupes, messages ou paquets émis ou permettant d'en accuser réception de façon sécurisée.

Un message sécurisé d'authentification et d'accusé de réception peut servir à

a) appliquer l'authentification, l'intégrité ou la non-répudiation de l'origine à des messages, paquets, groupes ou échanges;

b) assurer l'accusé de réception ou la non-répudiation de la réception sécurisés à des messages, paquets, groupes ou échanges sécurisés.

5.2 Champ d'application

Le message sécurisé d'authentification et d'accusé de réception (AUTACK) peut être utilisé pour le commerce tant national qu'international. Il est fondé sur la pratique universelle concernant l'administration, le commerce et le transport. Il ne dépend pas du type d'activité commerciale ou industrielle.

5.3 Principes

Les procédures de sécurité qui s'appliquent doivent être convenues par les partenaires commerciaux et définies dans un accord d'échange.

Le message sécurisé d'authentification et d'accusé de réception (AUTACK) permet de sécuriser d'autres structures EDIFACT (messages, paquets, groupes ou échanges) et de fournir un accusé de réception sécurisé relatif à des structures EDIFACT sécurisées. Il peut s'appliquer à des combinaisons de structures EDIFACT devant être sécurisées entre deux partenaires.

Les services de sécurité sont fournis par des mécanismes cryptographiques appliqués au contenu des structures EDIFACT initiales. Les résultats de ces mécanismes constituent le corps du message AUTACK et sont fournis par les données appropriées telles que les références des méthodes cryptographiques utilisées, les numéros de référence des structures EDIFACT et la date et l'heure des structures initiales.

Le message AUTACK doit utiliser les groupes d'en-tête et de fin de sécurité standardisés.

Le message AUTACK peut s'appliquer à un ou plusieurs messages, paquets ou groupes d'un ou de plusieurs échanges, ou à un ou plusieurs échanges.

5.3.1 Utilisation du message AUTACK pour remplir la fonction d'authentification

Un message AUTACK utilisé comme message d'authentification doit être émis par l'initiateur d'une ou de plusieurs structures EDIFACT acheminées séparément, ou par un intervenant habilité à agir au nom de l'initiateur. Son but est d'optimiser les services de sécurité définis dans la Partie 5 de l'ISO 9735, c'est-à-dire l'authenticité, l'intégrité, et la non-répudiation de l'origine des structures EDIFACT y étant associées.

Un message d'authentification AUTACK peut être mis en œuvre de deux façons. La première méthode véhicule les valeurs de hachage des structures EDIFACT référencées, sécurisées par le message AUTACK lui-même; la seconde n'utilise le message AUTACK que pour véhiculer les signatures numériques des structures EDIFACT référencées.

5.3.1.1 Authentification utilisant les valeurs de hachage des structures EDIFACT référencées

La structure EDIFACT sécurisée doit être référencée dans une occurrence du segment USX (références de sécurité). A chaque segment USX, doit correspondre au moins un segment USY (sécurité sur les références) qui contient le résultat de la sécurité, par exemple la valeur de hachage de la fonction de sécurisation appliquée à la structure EDIFACT référencée.

Les informations détaillées sur la fonction appliquée doivent être contenues dans le groupe d'en-tête de sécurité du message AUTACK. Les segments USY et USH de la structure EDIFACT référencée doivent être reliés à l'aide des éléments de données du numéro de référence de la sécurité dans les deux segments.

En dernier lieu, toutes les informations véhiculées dans le message AUTACK doivent être sécurisées à l'aide d'au moins une paire de groupes d'en-tête et de fin de sécurité.

NOTE AUTACK utilise le segment USX pour référencer un ou plusieurs messages, paquets ou groupes dans un ou plusieurs échanges ou pour référencer un échange complet. A chaque segment USX, un segment USY correspondant contient le résultat de hachage, la méthode d'authentification ou de non-répudiation appliquée à la structure EDIFACT référencée.

5.3.1.2 Authentification utilisant les signatures numériques de structures EDIFACT référencées

La structure EDIFACT sécurisée doit être référencée dans une occurrence du segment USX (références de sécurité). A chaque segment USX au moins un segment USY (sécurité sur les références) correspondant, qui contient la signature numérique de la structure EDIFACT référencée, doit être présent. Les informations détaillées sur la fonction de sécurité appliquée doivent être contenues dans le groupe d'en-tête de sécurité du message AUTACK. Du fait qu'une seule structure EDIFACT référencée peut être sécurisée plus d'une fois, le segment USY et le groupe d'en-tête de sécurité associés doivent être reliés à l'aide des éléments de données du numéro de référence des deux segments.

Si la signature numérique de la structure EDIFACT référencée est contenue dans le message AUTACK (plutôt qu'une simple valeur de hachage), ce dernier n'a pas besoin d'être sécurisé.

5.3.2 Utilisation du message AUTACK pour assurer la fonction d'accusé de réception

Un message AUTACK utilisé comme message d'accusé de réception doit être émis par le destinataire d'une ou de plusieurs structures EDIFACT sécurisées qu'il aura précédemment reçues ou par l'intervenant habilité à agir au nom du destinataire. Le but visé est de faciliter la confirmation de la réception, la validation de l'intégrité du contenu, la validation de l'intégralité et/ou la non-répudiation de réception de ses structures EDIFACT y étant associées.

La fonction d'accusé de réception ne doit être appliquée qu'à des structures EDIFACT. La structure EDIFACT sécurisée doit être référencée dans une occurrence du segment USX (références de sécurité). A chaque segment USX, doit correspondre au moins un segment USY (sécurité sur les références) qui contient soit la valeur de hachage, soit la signature numérique de la structure EDIFACT référencée. Le segment USY doit être relié à un groupe d'en-tête de sécurité de la structure EDIFACT référencée ou d'un message AUTACK le sécurisant, à l'aide de l'élément de données « numéro de référence de la sécurité ». L'en-tête de sécurité correspondante associé à la structure EDIFACT référencée contient les informations détaillées sur la fonction de sécurité, appliquée à la structure EDIFACT référencée par l'émetteur du message initial.

A la dernière étape de la génération du message d'accusé de réception, toutes les informations véhiculées dans le message AUTACK doivent être sécurisées à l'aide d'au moins une paire de groupes d'en-tête et de fin de sécurité.

Le message AUTACK peut également servir d'accusé de non-réception au cas où la vérification des résultats de sécurité poserait des difficultés.

NOTE L'accusé de réception ne prend son sens que pour les structures EDIFACT sécurisées. La sécurisation des structures EDIFACT s'effectue par l'utilisation soit de segments de sécurité intégrés (voir Partie 5 de l'ISO 9735), soit par le message d'authentification AUTACK.

Pour éviter des boucles infinies, un message AUTACK utilisé pour assurer la fonction d'accusé de réception ne doit pas obliger son destinataire à renvoyer un message d'accusé de réception AUTACK.

5.4 Définition du message

5.4.1 Précisions sur les segments de données

0010 **UNH, En-tête de message**

Segment de service débutant et identifiant de façon unique un message.

Le code du type de message pour le message Authentification et accusé de réception est AUTACK.

L'élément de données « Identification de la sous-fonction du type de message » doit être utilisé pour indiquer si le message AUTACK doit remplir la fonction du message AUTACK d'authentification, d'accusé de réception ou de refus d'accusé réception.

NOTE Les messages conformes à ce document doivent contenir les données suivantes dans la composite S009 du segment UNH.

Elément de Données	0065	AUTACK
	0052	4
	0054	1
	0051	UN

0020 **Groupe de segments 1: USH-USA-SG2 (groupe d'en-tête de sécurité)**

Groupe de segments identifiant le service de sécurité et les mécanismes de sécurité appliqués et contenant les données nécessaires à l'exécution des calculs de validation (comme défini dans la Partie 5 de l'ISO 9735). Ce groupe de segments doit indiquer le service et le (les) algorithme(s) appliqué(s) au message AUTACK ou à la structure EDIFACT référencée.

Chaque groupe d'en-tête de sécurité doit être relié à un groupe de fin de sécurité et certains peuvent être, de surcroît, reliés aux segments USY.

0030 **USH, En-tête de sécurité**

Segment indiquant un service de sécurité appliqué au message/paquet précisé dans ce segment ou à la structure EDIFACT référencée (comme défini dans la Partie 5 de l'ISO 9735).

L'élément de données de service de la sécurité doit indiquer la fonction de sécurité appliquée au message AUTACK ou à la structure EDIFACT référencée :

— services de sécurité: l'authentification de l'origine et la non-répudiation d'origine du message ne doivent être utilisés que pour le message AUTACK lui-même.

— services de sécurité: l'intégrité de la structure EDIFACT référencée, l'authentification et la non-répudiation de la structure EDIFACT référencée ne doivent être utilisées par l'émetteur que pour sécuriser les structures EDIFACT référencées du message AUTACK.

— services de sécurité: l'authentification de la réception et la non-répudiation de la réception ne doivent être utilisées par le récepteur de structures EDIFACT sécurisées que pour sécuriser l'accusé de réception.

Le domaine d'application du service de sécurité doit être précisé, comme défini dans la Partie 5 de l'ISO 9735. Dans un message AUTACK, quatre domaines d'application peuvent exister :

— les deux premiers sont tels que définis dans la section 5 de la Partie 5 de l'ISO 9735.

— le troisième comprend l'ensemble de la structure EDIFACT, dans lequel le domaine d'application de la sécurité commence à partir du premier caractère du message, paquet, groupe ou échange (à savoir un « U ») et se termine au dernier caractère compris du message, paquet, groupe ou échange.

— le quatrième est défini par l'utilisateur, l'application de la sécurité dans ce domaine étant définie en accord entre l'émetteur et le récepteur.

0040 **USA, Algorithme de sécurité**

Segment identifiant un algorithme de sécurité, l'utilisation technique qui en est faite, et contenant les paramètres techniques requis (comme défini dans la Partie 5 de l'ISO 9735).

0050 **Groupe de segments 2: USC-USA-USR (groupe du certificat)**

Groupe de segments contenant les données nécessaires à la validation des méthodes de sécurité appliquées au message/paquet, lorsque des algorithmes asymétriques sont utilisés (comme défini dans la Partie 5 de l'ISO 9735).

0060 **USC, Certificat**

Segment contenant, par exemple, l'identité du propriétaire du certificat et identifiant l'autorité de certification qui a produit le certificat (comme défini dans la Partie 5 de l'ISO 9735).

0070 **USA, Algorithme de sécurité**

Segment identifiant un algorithme de sécurité, l'utilisation technique qui en est faite et contenant les paramètres techniques requis (comme défini dans la Partie 5 de l'ISO 9735).

0080 **USR, Résultat de la sécurité**

Segment contenant le résultat des fonctions de sécurité appliquées au certificat par l'autorité de certification (comme défini dans la Partie 5 de l'ISO 9735).

0090 **USB, Identification des données sécurisées**

Ce segment doit contenir l'identification de l'émetteur de l'échange et du destinataire de l'échange, un horodatage de sécurité associé du message AUTACK et doit indiquer si un accusé de réception sécurisé émanant du destinataire de ce même message est requis ou non. Dans l'affirmative, l'émetteur du message doit s'attendre à ce qu'un message d'accusé de réception AUTACK lui soit retourné par le destinataire du message.

L'émetteur de l'échange et le destinataire de l'échange doivent faire référence, dans le segment USB, à l'émetteur et au destinataire de l'échange dans lequel le message AUTACK est présent, afin de sécuriser ces informations.

0100 **Groupe de segments 3: USX-USY**

Ce groupe de segments doit servir à identifier un intervenant impliqué dans le processus de sécurité et à donner les informations concernant la sécurité de la structure EDIFACT référencée.

0110 **USX, Références de la sécurité**

Ce segment doit contenir les références renvoyant à l'intervenant impliqué dans le processus de sécurité.

L'élément de données composite «Date et heure de la sécurité» peut contenir la date et l'heure initiales de la production de la structure EDIFACT référencée.

Si l'élément de données 0020 est présent et qu'aucun des éléments: 0048, 0062 et 0800 ne le sont, l'ensemble de l'échange est référencé.

Si les éléments de données 0020 et 0048 sont présents et aucun des éléments: 0062 et 0800 ne le sont, le groupe est référencé.

0120 **USY, Sécurité sur les références**

Segment contenant un lien à un groupe d'en-tête de sécurité et le résultat des services de sécurité appliqués à la structure EDIFACT référencée comme précisé dans le groupe d'en-tête de sécurité relié.

Lorsque les structures EDIFACT référencées sont sécurisées par le même service de sécurité, avec les mêmes paramètres de sécurité associés, de nombreux segments USY peuvent être reliés au même groupe d'en-tête de sécurité. Dans ce cas, la valeur du lien entre le groupe d'en-tête de sécurité et les segments USY associés doit être la même. Lorsque le message AUTACK est utilisé pour assurer la fonction d'accusé de réception, le groupe d'en-tête de sécurité correspondant doit être soit l'un de la structure EDIFACT référencée, soit l'un d'un message AUTACK utilisé pour indiquer la structure EDIFACT référencée avec la fonction d'authentification.

Dans un segment USY, l'élément de données 0534 doit être identique à la valeur de cet élément 0534 contenu dans le segment USH correspondant

— du message AUTACK courant, si la fonction d'authentification est utilisée (services de sécurité: authenticité de l'origine de la structure EDIFACT référencée, intégrité de la structure EDIFACT référencée ou non-répudiation de l'origine de la structure EDIFACT référencée);

— de la structure EDIFACT référencée elle-même ou d'un message AUTACK fournissant la structure EDIFACT référencée avec la fonction d'authentification, si la fonction d'accusé de réception est utilisée (services de sécurité: non-répudiation de réception ou authentification de réception).

0130 **Groupes de segments 4: UST-USR (groupe de fin de sécurité)**

Groupe de segments contenant un lien avec le groupe de segments d'en-tête et le résultat des fonctions de sécurité appliquées au message/paquet (comme défini dans la Partie 5 de l'ISO 9735).

Le segment USR peut être omis si le groupe de fin de sécurité est relié à un groupe d'en-tête de sécurité associé à une structure EDIFACT référencée. Dans ce cas, les résultats correspondants de la fonction de sécurité doivent se trouver dans les segments USY qui sont liés au groupe d'en-tête de sécurité approprié.

0140 **UST, Fin de sécurité**

Segment établissant un lien entre le groupe de segments d'en-tête et de fin de sécurité et indiquant le nombre de segments de sécurité contenant ces groupes (comme défini dans la Partie 5 de l'ISO 9735).

0150 **USR, Résultat de la sécurité**

Segment contenant le résultat des fonctions de sécurité appliquées au message/paquet comme défini dans le groupe d'en-tête de sécurité relié (comme défini dans la Partie 5 de l'ISO 9735). Dans ce segment, le résultat de la sécurité doit être appliqué au message AUTACK lui-même.

0160 **UNT, Fin du message**

Segment de service terminant un message, indiquant le nombre total de segments dans le message et le numéro de référence de contrôle du message.

5.4.2 Structure du message

5.4.2.1 Table des segments

POS	Etiquette	Nom	S	R	Notes
0010	UNH	En-tête de message	M	1	
0020	----	Groupe de segments 1---------	M	99	-------+
0030	USH	En-tête de sécurité	M	1	|
0040	USA	Algorithme de sécurité	C	3	|
					|
0050	-----	Groupe de segments 2---------	C	2	----+ |
0060	USC	Certificat	M	1	| |
0070	USA	Algorithme de sécurité	C	3	| |
0080	USR	Résultat de la sécurité	C	1	----+--+
0090	USB	Identification des données sécurisées	M	1	
0100	-----	Groupe de segments 3---------	M	9999	----+
0110	USX	Références de la sécurité	M	1	|
0120	USY	Sécurité sur les références	M	9	----+
0130	-----	Groupe de segments 4---------	M	99	----+
0140	UST	Fin de sécurité	M	1	|
0150	USR	Résultat de la sécurité	C	1	----+
0160	UNT	Fin de message	M	1	

NOTE Le corps du message AUTACK comprend le segment UNB et le groupe de segments 3.