NORME INTERNATIONALE

ISO 9735-9

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

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

Part 9: Security key and certificate management message (message type — KEYMAN)

Numéro de référence
ISO 9735-9:1999(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 9735-9 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 H sont données uniquement 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 gérer les clés et les certificats de sécurité.

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

1 Domaine d'application

La présente partie de l'ISO 9735 est destinée à la sécurité EDIFACT par lots et définit le message Gestion de clés et de certificats de sécurité KEYMAN.

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/CEI 9594-8:—[1)], *Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — L'Annuaire: Cadre d'authentification [Recommandation UIT-T X 509 (1997)]*.

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, s'appliquent.

5 Règles d'utilisation du message Gestion des clés et de certificats de sécurité

5.1 Définition fonctionnelle

KEYMAN est un message assurant la gestion de clés et de certificats de sécurité. Une clé peut être une clé secrète utilisée avec des algorithmes symétriques ou une clé publique ou privée utilisée avec des algorithmes asymétriques.

5.2 Champ d'application

Le message Gestion de clés et de certificats de sécurité (KEYMAN) 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

Ce message peut servir à demander ou à remettre des clés de sécurité, des certificats, ou des chemins de certification (ce principe couvre la demande d'autres activités portant sur la gestion de clés et de certificats, par exemple le renouvellement, le remplacement ou la révocation de certificats et la fourniture d'autres informations telles que le statut d'un certificat). Il peut servir à remettre des listes de certificats (par exemple, indiquer les certificats qui ont été révoqués). Le message KEYMAN peut être sécurisé à l'aide des groupes de segments d'en-tête et de fin de sécurité. Les structures des groupes de segments d'en-tête et de fin de sécurité sont définis dans la Partie 5 de l'ISO 9735.

Un message de gestion de clés et de certificats de sécurité peut servir à

a) demander des actions concernant des clés et des certificats

b) fournir des clés, des certificats et des informations s'y rapportant.

---

1) À publier. (Révision de l'ISO/CEI 9594-8:1995)

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 Gestion de clés et de certificats de sécurité est KEYMAN.

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

Elément de données	0065	KEYMAN
	0052	4
	0054	1
	0051	UN

0020 **Groupe de segments 1: USE-USX-SG2**

Groupe de segments contenant toutes les informations nécessaires pour véhiculer les demandes, remises et avis de clés, de certificats ou de chemins de certification.

0030 **USE, relation avec un message de sécurité**

Segment identifiant une relation à un message antérieur, telle qu'une demande d'un message KEYMAN.

0040 **USX, Références de la sécurité**

Segment identifiant un lien avec un message antérieur, tel qu'une demande. L'élément de données composite «Date et heure de la sécurité» peut contenir la date et l'heure de la production d'origine du message référencé.

0050 **Groupe de segments 2: USF-USA-SG3**

Groupe de segments contenant une seule clé, un seul certificat ou groupe de certificats formant un chemin de certification.

0060 **USF, Fonction de gestion de la clé**

Segment identifiant la fonction du groupe qu'il déclenche, soit une demande ou une remise. S'il est utilisé pour indiquer des éléments des chemins de certification, le numéro de séquence du certificat doit indiquer la position du certificat qui suit dans le chemin de certification. Il peut être utilisé seul pour la restitution de listes, sans qu'aucun certificat ne soit présent. Plusieurs différents segments USF peuvent se trouver dans le même message, si plus d'une clé ou d'un certificat est traité. Cependant, les fonctions de demande et les fonctions de remise ne doivent pas être mélangées. Le segment USF peut également préciser la fonction du filtre utilisé pour les champs binaires du segment USA qui suit immédiatement ce segment.

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). Ce segment doit être utilité pour des demandes, une suspension ou une remise de clés symétriques. Il peut également servir à demander une paire de clés asymétriques.

0080 **Groupe de segments 3: USC-USA-USR**

Groupe de segments contenant les dates 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). Ce groupe doit être utilisé dans la demande ou la remise de clés et de certificats.

Ou bien la totalité du groupe de segments du certificat (y compris le segment USR) ou les seuls éléments de données nécessaires à identifier de façon non ambiguë la paire de clés asymétriques utilisée, doit être présente dans le segment USC. La présence d'un certificat dans sa totalité peut être évitée si le certificat a déjà été échangé entre les deux intervenants, ou il peut être extrait d'une base de données.

Si l'on veut faire référence à un certificat non EDIFACT (tel que X.509), la syntaxe et la version du certificat doivent être identifiées dans l'élément de données 0545 du segment USC. Ces certificats peuvent être véhiculés dans un paquet EDIFACT.

0090 **USC, Certificat**

Segment contenant les justificatifs 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). Ce segment doit être utilisé pour des demandes de certificat concernant un renouvellement ou des demandes de clés asymétriques telles qu'une suspension ainsi que pour des remises de certificats.

0100 **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). Ce segment doit être utilisé pour des demandes de certificats concernant l'enregistrement de justificatifs et pour des remises de certificats.

0110 **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). Ce segment doit être utilisé pour la validation des certificats ou les remises de certificats.

0120 **Groupe de segments 4: USL-SG5**

Groupe de segments contenant les listes de certificats ou de clés publiques. Ce groupe doit être utilisé pour regrouper des certificats de statut similaire, c'est-à-dire qui sont toujours en cours de validité, ou peuvent ne plus l'être à cause d'une raison quelconque.

0130 **USL, Statut de la liste de sécurité**

Segment identifiant des éléments en cours de validité, révoqués, inconnus ou suspendus. Il peut s'agir de certificats (par exemple, en cours de validité, révoqués) ou de clés publiques (par exemple, en cours de validité ou interrompues). Ce message peut comporter plusieurs différents segments USL, si la remise implique plus d'une liste de certificats ou de clés publiques. Ces différentes listes peuvent être identifiées par les paramètres de la liste.

0140 **Groupe de segments 5: USC-USA-USR**

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). Ce groupe doit être utilisé dans la remise de listes de clés ou de certificats de statut similaire.

0150 **USC, Certificat**

Segment contenant les justificatifs du propriétaire du certificat et identifiant l'autorité de certification qui a produit le certificat (comme défini dans la Partie 5). Ce segment doit être utilisé, soit dans la totalité du certificat, avec, en plus, les segments USA et USR. Il peut aussi indiquer le numéro de référence du certificat ou le nom de la clé. Dans ce cas le message doit être signé en utilisant les groupes de segments d'en-tête et de fin de sécurité.

0160 **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). S'il est nécessaire d'indiquer les algorithmes utilisés avec un certificat, ce segment doit être utilisé.

0170 **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). S'il est nécessaire de signer un certificat, ce segment doit être utilisé.

0180 **UNT, Fin de 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 Index des segments de données

Etiquette	Nom
UNH	En-tête de message
UNT	Fin de message
USA	Algorithme de sécurité
USC	Certificat
USE	Relation avec un message de sécurité
USF	Fonction de gestion de la clé
USL	Statut de la liste de sécurité
USR	Résultat de la sécurité
USX	Références de la sécurité

5.4.3 Structure du message

5.4.3.1 Segment table

POS	Etiquette	Nom	S	R	
0010	UNH	En-tête de message	M	1	
0020	-----	Groupe de segments 1 --------------	C	999	--------+
0030	USE	Relation avec un message de sécurité	M	1	|
0040	USX	Références de la sécurité	C	1	|
					|
0050	-----	Groupe de segments 2 --------------	M	9	----+ |
0060	USF	Fonction de gestion de la clé	M	l	| |
0070	USA	Algorithme de sécurité	C	1	| |
					| |
0080	-----	Groupe de segments 3 --------------	C	1	-+ | |
0090	USC	Certificat	M	1	| | |
0100	USA	Algorithme de sécurité	C	3	| | |
0110	USR	Résultat de la sécurité	C	1	--------+
0120	-----	Groupe de segments 4 --------------	C	99	--------+
0130	USL	Statut de la liste de sécurité	M	1	|
					|
0140	-----	Groupe de segments 5 --------------	M	9999	----+ |
0150	USC	Certificat	M	1	| |
0160	USA	Algorithme de sécurité	C	3	| |
0170	USR	Résultat de la sécurité	C	1	--------+
0180	UNT	Fin de message	M	1	

Annexe A
(normative)

Définitions
Addendum — à ajouter à l'annexe A de la Partie 1 une fois approuvée —

A.1
chemin de certification
séquence ordonnée de certificats d'objets dans l'Arbre des informations de l'annuaire qui, accompagnée de la clé publique de l'objet d'origine dans le chemin, peut être traitée pour obtenir celle de l'objet final dans ce chemin. (ISO 9594-8) [1]