

	<p>Elektronická výměna dat pro správu, obchod a dopravu (EDIFACT) - Pravidla syntaxe aplikační úrovně (Číslo verze syntaxe: 4, číslo vydání syntaxe: 1) - Část 9: Správa bezpečnostních klíčů a certifikátů (zpráva KEYMAN)</p>	<p>ČSN ISO 9735-9  97 9735</p>
---	---	--

Electronic data interchange for administration, commerce and transport (EDIFACT) - Application level syntax rules

(Syntax version number: 4, Syntax release number: 1) -

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

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, numéro d'édition de syntaxe: 1) -

Partie 9: Clé de sécurité et message de gestion de certificat (type de message - KEYMAN)

Tato norma je českou verzí mezinárodní normy ISO 9735-9:2002. Mezinárodní norma ISO 9735-9:2002 má status české technické normy.

This standard is the Czech version of the International Standard ISO 9735-9:2002. The International Standard ISO 9735-9:2002 has the status of a Czech Standard.

© Český normalizační institut,

2003

Podle zákona č. 22/1997 Sb. smějí být české technické normy rozmnožovány a rozšiřovány jen se souhlasem Českého normalizačního institutu.

**67055**

## Citované normy

ISO 9735-1:2002 zavedena v ČSN ISO 9735-1:2003 (97 9735) Elektronická výměna dat pro správu, obchod a dopravu (EDIFACT) - Pravidla syntaxe aplikační úrovně (číslo verze syntaxe: 4, číslo vydání syntaxe: 1) - Část 1: Pravidla syntaxe společná pro všechny části

ISO 9735-2:2002 zavedena v ČSN ISO 9735-2:2003 (97 9735) Elektronická výměna dat pro správu, obchod a dopravu (EDIFACT) - Pravidla syntaxe aplikační úrovně (číslo verze syntaxe: 4, číslo vydání syntaxe: 1) - Část 2: Pravidla syntaxe specifická pro dávkovou EDI

ISO 9735-5:2002 bude zavedena v ČSN ISO 9735-5:2004 (97 9735) Elektronická výměna dat pro správu, obchod a dopravu (EDIFACT) - Pravidla syntaxe aplikační úrovně (číslo verze syntaxe: 4, číslo vydání syntaxe: 1) - Část 5: Pravidla bezpečnosti pro dávkovou EDI (autentičnost, integrita a nepopření původu)

ISO 9735-10:2002 bude zavedena v ČSN ISO 9735-10:2004 (97 9735) Elektronická výměna dat pro správu, obchod a dopravu (EDIFACT) - Pravidla syntaxe aplikační úrovně (číslo verze syntaxe: 4, číslo vydání syntaxe: 1) - Část 10: Syntaktické služební sborníky

## Vypracování normy

Zpracovatel: Ing. Miroslav Kyncl, CSc., IČO 42505623

Technická normalizační komise: TNK 42 Výměna dat

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

Strana 3

---

MEZINÁRODNÍ NORMA

**Elektronická výměna dat pro správu, obchod a dopravu**

**ISO**

**9735-9**

**(EDIFACT) - Pravidla syntaxe aplikační úrovně**

Druhé vydání

**(Číslo verze syntaxe: 4, číslo vydání syntaxe: 1) -**  
07-01

2002-

**Část 9: Správa bezpečnostních klíčů a certifikátů**  
**(zpráva KEYMAN)**

ICS 35.240.60

Deskriptory: management, commerce, transportation, computer applications, electronic documents, administrative documents, commercial documents, messages, data processing, information interchange, protection of information, security techniques, algorithms.

#### Odmítnutí odpovědnosti za manipulaci s PDF

Tento soubor PDF může obsahovat vložené typy písma. V souladu s licenční politikou Adobe tento soubor lze tisknout nebo prohlížet, avšak nesmí být editován, kromě těch vložených typů písma, které nepodléhají licenci a jsou instalovány v počítači, na kterém se editace provádí. Při používání tohoto souboru jsou jeho uživatelé odpovědní za to, že nebude porušena licenční politika Adobe. Ústřední sekretariát ISO nepřijímá za její porušení žádnou odpovědnost.

Adobe je obchodní značka „Adobe Systems Incorporated“.

Podrobnosti o softwarových produktech, které vytvářejí tento soubor PDF, lze najít ve všeobecných informacích, které jsou k němu přiloženy; parametry na vytváření PDF jsou optimalizovány pro tisk. Soubor je upraven tak, aby byl použitelný členskými organizacemi ISO. V případě nepravděpodobné události a problému, který se k ní vztahuje, informujte Ústřední sekretariát ISO. Jeho adresa je uvedena níže.

Všechna práva vyhrazena. Není-li uvedeno jinak, nesmí být žádná část této publikace reprodukována nebo zpracována jakoukoli jinou formou, jako jsou například elektronické nebo mechanické prostředky, včetně fotokopíí a mikrofilmu, bez písemného povolení ISO; povolení lze vyžádat na níže uvedené adrese nebo u členské národní organizace v zemi žadatele.

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](mailto:copyright@iso.ch)

Web [www.iso.ch](http://www.iso.ch)

Strana 4

---

Obsah

Strana

Předmluva

.....  
..... 5

Úvod

.....  
..... 6

**1** Předmět  
normy

.....  
..... 6

**2**

Shoda	6
<b>3</b> Normativní odkazy	6
<b>4</b> Termíny a definice	7
<b>5</b> Pravidla pro použití zprávy správa bezpečnostních klíčů a certifikátů	7
<b>Příloha A</b> (informativní) Funkce KEYMAN	11
<b>Příloha B</b> (informativní) Bezpečnostní techniky použité u zpráv KEYMAN	14
<b>Příloha C</b> (informativní) Použití skupin segmentů ve zprávách KEYMAN	15
<b>Příloha D</b> (informativní) Model správy klíčů	17
<b>Příloha E</b> (informativní) Příklady správy klíčů a certifikátů	19

## Předmluva

ISO (Mezinárodní organizace pro normalizaci) je celosvětovou federací národních normalizačních orgánů (členů ISO). Mezinárodní normy obvykle připravují technické komise ISO. Každý člen ISO, který se zajímá o předmět, pro který byla vytvořena technická komise, má právo být v této technické komisi zastoupen. Práce se zúčastňují také vládní i nevládní mezinárodní organizace, s nimiž ISO navázala pracovní styk. ISO úzce spolupracuje s Mezinárodní elektrotechnickou komisí (IEC) ve všech záležitostech normalizace v elektrotechnice.

Mezinárodní normy se navrhují v souladu s pravidly uvedenými ve směrnících ISO/IEC, část 3.

Hlavní činností technických komisí je příprava mezinárodních norem. Návrhy mezinárodních norem přijaté technickými komisemi se rozesílají členům ISO k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75 % hlasujících členů.

Upozorňuje se na možnost, že některé prvky této části ISO 9735 mohou být předmětem patentových

práv. ISO neodpovídá za uvedení některého nebo všech takových patentových práv.

ISO 9735-9 byla vypracována technickou komisí ISO/TC 154, *Procesy, datové prvky a doklady v obchodě, průmyslu a ve správě* ve spolupráci s UN/CEFACT prostřednictvím Společné pracovní skupiny pro syntaxi (JSWG).

Toto druhé vydání ruší a nahrazuje první vydání (ISO 9735-9:1999). Avšak dočasně je zachována ISO 9735:1988 a její Dodatek 1:1992 z důvodů uvedených v kapitole 2.

Z důvodů aktualizace byly z této části a ze všech ostatních částí série ISO 9735 odstraněny syntaktické služební sborníky. Ty jsou nyní soustředěny v nové části, ISO 9735-10.

V době vydání ISO 9735-1:1998 byla ISO 9735-10 určena jako část pro „Pravidla bezpečnosti pro interaktivní EDI“. Ta byla později stažena pro nedostatek podpory uživatelů a výsledkem je, že všechny odkazy na titul „Pravidla bezpečnosti pro interaktivní EDI“ byly z tohoto druhého vydání ISO 9735-9 odstraněny.

Definice ze všech částí série ISO 9735 byly soustředěny a zařazeny do ISO 9735-1.

ISO 9735 se společným názvem *Elektronická výměna dat pro správu, obchod a dopravu (EDIFACT) - Pravidla syntaxe aplikační úrovně (číslo verze syntaxe: 4, číslo vydání syntaxe: 1)* sestává z částí:

- Část 1: Pravidla syntaxe společná pro všechny části
- Část 2: Pravidla syntaxe specifická pro dávkovou EDI
- Část 3: Pravidla syntaxe specifická pro interaktivní EDI
- Část 4: Syntaktické a služební hlášení pro dávkovou EDI (zpráva CONTRL)
- Část 5: Pravidla bezpečnosti pro dávkovou EDI (autentičnost, integrita a nepopření původu)
- Část 6: Bezpečnostní autentizace a potvrzení (zpráva AUTACK)
- Část 7: Pravidla bezpečnosti pro dávkovou EDI (důvěrnost)
- Část 8: Přidružená data v EDI
- Část 9: Správa bezpečnostních klíčů a certifikátů (zpráva KEYMAN)
- Část 10: Syntaktické služební sborníky

Později mohou být doplněny další části.

Přílohy A až E této části ISO 9735 jsou pouze informativní.

## Úvod

Tato část ISO 9735 obsahuje pravidla na aplikační úrovni pro strukturování dat při výměně

elektronických zpráv v otevřeném prostředí založená na požadavcích dávkového zpracování. Tato pravidla byla schválena Evropskou hospodářskou komisí OSN (OSN/EHK) jako pravidla syntaxe pro elektronickou výměnu dat pro správu, obchod a dopravu (EDIFACT) a jsou součástí Sborníku OSN pro výměnu dat v obchodě (United Nations Trade Data Interchange Directory - UNTDID), který také obsahuje příručky pro navrhování jak dávkových, tak i interaktivních zpráv.

Komunikační protokoly a specifikace nejsou předmětem této části ISO 9735.

Toto je nová část, která byla připojena k ISO 9735. Poskytuje volitelnou možnost správy bezpečnostních klíčů a certifikátů.

# 1 Předmět normy

Tato část ISO 9735 pro dávkovou EDI specifikuje zprávu KEYMAN Správa bezpečnostních klíčů a certifikátů.

---

-- Vynechaný text --