



中华人民共和国国家标准

GB/T 14805.7—1999
idt ISO 9735-7:1998

用于行政、商业和运输业电子数据交换的 应用级语法规则(语法版本号:4) 第7部分:批式电子数据交换安全规则 (保密性)

**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)**

1999-11-11 发布

2000-05-01 实施

国家质量技术监督局 发布

目 次

前言	I
ISO 前言	II
ISO 引言	III
1 范围	1
2 一致性	1
3 引用标准	1
4 定义	1
5 批式 EDI 保密性规则	1
5.1 EDIFACT 保密性	1
5.2 使用的原则	6
附录 A(标准的附录) 语法服务目录(段、复合数据元和简单数据元)	7
附录 B(提示的附录) 报文保护示例	9
附录 C(提示的附录) 处理示例	11
附录 D(提示的附录) 保密性服务和算法	12

前 言

本标准等同采用 ISO 9735-7:1998《用于行政、商业和运输业电子数据交换的应用级语法规则(语法版本号:4) 第7部分:批式电子数据交换安全规则(保密性)》。

GB/T 14805 系列标准在《用于行政、商业和运输业电子数据交换的应用级语法规则(语法版本号:4)》的总标题下,包括下列 10 个部分:

- 第 1 部分:各部分公用的语法规则及每部分的语法服务目录
- 第 2 部分:批式电子数据交换专用的语法规则
- 第 3 部分:交互式电子数据交换专用的语法规则
- 第 4 部分:批式电子数据交换语法和服务报告报文(报文类型为 CONTRL)
- 第 5 部分:批式电子数据交换安全规则(真实性、完整性和源抗抵赖性)
- 第 6 部分:安全鉴别和确认报文(报文类型为 AUTACK)
- 第 7 部分:批式电子数据交换安全规则(保密性)
- 第 8 部分:电子数据交换中的相关数据
- 第 9 部分:密钥和证书管理报文(报文类型为 KEYMAN)
- 第 10 部分:交互式电子数据交换安全规则

将来还有可能增加新的部分。

GB/T 14805.×—1999 对应于 ISO 9735 第四版,它的发布与实施,不影响我国 1993 年根据 ISO 9735:1988 制定的国家标准 GB/T 14805—1993。

本标准由中华人民共和国国家信息化办公室提出。

本标准由全国文件格式和数据元标准化技术委员会、全国信息技术标准化技术委员会归口。

本标准起草单位:邮电部数据通信技术研究所以、电子工业部标准化研究所、中国标准化与信息分类编码研究所。

本标准主要起草人:张泽忠、吴志刚、王颜尊、刘碧松、张萍、徐冬梅、王欣、苑琳。

ISO 前言

ISO(国际标准化组织)是一个世界性的各国标准机构(ISO 国家成员体)联盟。国际标准的制定工作一般通过 ISO 技术委员会完成。对某个已建立的技术委员会的项目感兴趣的每个成员体,有权对该技术委员会表述意见。任何与 ISO 有联络关系的官方和非官方的国际组织都可直接参与制定国际标准。ISO 与 IEC(国际电工委员会)在电工技术标准的所有领域密切合作。

由技术委员会正式通过的国际标准草案在被 ISO 理事会接受为国际标准之前,须分发到各成员体进行表决,按照 ISO 的工作程序,在得到至少 75%的成员体投票赞成之后,该标准草案才成为国际标准。

本国际标准 ISO 9735 第四版由联合国欧洲经济委员会第四工作组(UN/ECE/WP.4)起草(作为 UN/EDIFACT 的组成部分),由 ISO/TC 154(行政、商业和工业中的单证和数据元)通过“快速表决程序”采纳为现行标准。

ISO/IEC 9735 在《联合国用于行政、商业和运输业的电子数据交换应用级语法规则》的总标题下由下列几部分组成:

- ISO 9735-1 各部分公用的语法规则及每部分的语法服务目录
- ISO 9735-2 批式电子数据交换专用的语法规则
- ISO 9735-3 交互式电子数据交换专用的语法规则
- ISO 9735-4 批式电子数据交换语法和服务报告报文(报文类型为 CONTRL)
- ISO 9735-5 批式电子数据交换安全规则(真实性、完整性和源抗抵赖性)
- ISO 9735-6 安全鉴别和确认报文(报文类型为 AUTACK)
- ISO 9735-7 批式电子数据交换安全规则(保密性)
- ISO 9735-8 电子数据交换中的相关数据
- ISO 9735-9 密钥和证书管理报文(报文类型为 KEYMAN)
- ISO 9735-10 交互式电子数据交换安全规则

将来还有可能增加新的部分。

ISO 引言

根据批式或交互式处理的需求,本标准包含了用于结构化在开放环境中交换的电子报文中的数据的应用级规则。联合国欧洲经济委员会(UN/ECE)已经同意把这些规则作为用于行政、商业和运输业电子数据交换(EDIFACT)的应用级语法规则。这些规则是联合国贸易数据交换目录(UNTDID)的一部分。UNTDID 还包含批式和交互式报文设计指南。

通讯规范及协议不在本标准的范围之内。

本标准是 ISO 9735 新增加的部分。它提供了 EDIFACT 结构(报文、包、组或交换)保密性的可选能力。

中华人民共和国国家标准

用于行政、商业和运输业电子数据交换的 应用级语法规则(语法版本号:4) 第7部分:批式电子数据交换安全规则 (保密性)

GB/T 14805.7—1999
idt ISO 9735-7:1998

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)

1 范围

本标准按照所建立的安全机制规定了报文/包级、组级和交换级的保密性。

2 一致性

与一个标准一致意味着支持其所有需求,包括所有选项。如果不是所有选项都被支持,则任何一致性声明都应包含一个说明,用于标识那些被声明为与其一致的选项。

如果所交换的数据的结构和表示符合本标准中规定的语法规则,则这些数据处于一致性状态。

当支持本标准的设备能创建和/或解释其结构和表示与本标准一致的数据时,这些设备处于一致性状态。

与本标准的一致应包含与 GB/T 14805.1、GB/T 14805.2 和 GB/T 14805.5 的一致。

当在本标准中标识出在相关标准中定义的条款时,这些条款应构成一致性判定条件的组成部分。

3 引用标准

下列标准所包含的条文,通过在本标准中引用而构成本标准的条文。本标准出版时,所示版本均为有效。所有标准都会被修订,使用本标准的各方应探讨使用下列标准最新版本的可能性。

ISO/IEC 10181-5:1996 信息技术 开放系统中的安全框架 第5部分:保密性

4 定义

本标准采用的定义见 GB/T 14805.1—1999 的附录 A 和 GB/T 14805.5—1999 的附录 A。

5 批式 EDI 保密性规则

5.1 EDIFACT 保密性

GB/T 14805.5—1999 附录 C 和附录 D 描述了与 EDIFACT 数据传送有关的安全威胁及针对这些威胁的安全服务。

本条描述了向 EDIFACT 结构提供保密性安全服务的解决方案。