ICS 35.240.60
L 70

中华人民共和国国家标准

GB/T 14805.9—2001
idt ISO 9735-9:1999

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9部分:安全密钥和证书管理报文(报文类型为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)

2001-04-09 发布　　2001-10-01 实施

国家质量技术监督局 发布

目　　次

前言 …… I
ISO 前言 …… II
引言 …… III
1　范围 …… 1
2　一致性 …… 1
3　引用标准 …… 1
4　定义 …… 2
5　安全密钥和证书管理报文的使用规则 …… 2
附录 A(标准的附录)　定义 …… 5
附录 B(标准的附录)　语法服务目录(段、复合数据元和简单数据元) …… 5
附录 C(提示的附录)　KEYMAN 功能 …… 10
附录 D(提示的附录)　应用于 KEYMAN 报文的安全技术 …… 13
附录 E(提示的附录)　KEYMAN 报文中段组的使用 …… 14
附录 F(提示的附录)　密钥管理模式 …… 15
附录 G(提示的附录)　语法服务代码目录 …… 16
附录 H(提示的附录)　密钥和证书管理示例 …… 16

前　言

本标准等同采用 ISO 9735-9:1999《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 9 部分:安全密钥和证书管理报文(报文类型为 KEYMAN)》。

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 9 个部分:

第 1 部分:公用的语法规则及语法服务目录

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:安全密钥和证书管理报文(报文类型为 KEYMAN)

将来还有可能增加新的部分。

GB/T 14805 系列标准对应于 ISO 9735 第 4 版。

虽然 ISO 9735:1998 替代了早期各版,但根据 ISO 9735:1998 的有关规定,用户仍可使用早期各版,有鉴于此,我国于 1993 年根据 ISO 9735 的 1988 版、1990 版和 1992 版制定的国家标准 GB/T 14805—1993亦可在今后一段时间内继续使用。因此,本系列标准的发布与实施,不替代 GB/T 14805—1993。

在本标准中,附录 A 和附录 B 是标准的附录,是本标准不可分割的组成部分。附录 C 到附录 H 是提示的附录。

本标准由中国标准研究中心提出。

本标准由全国电子业务标准化技术委员会归口。

本标准起草单位:中国标准研究中心、中国人民银行、四川大学信息安全研究所。

本标准主要起草人:李颖、刘碧松、陈耀东、周安民、胡涵景、邓洁等。

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,有权对该项目表述意见。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)在电工技术标准化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 9735-9 由联合国欧洲经济委员会(UN/ECE)的贸易部门起草(作为 UN/EDIFACT 的组成部分),并由 ISO/TC 154(行政、商业和工业中的单证和数据元技术委员会)通过"快速表决程序"采纳为现行标准。

鉴于本标准替代了早期各版,并在交换头(UNB)段的必备型数据元 0002(语法版本号)中用"4"来标识本版本,因此,继续使用早期发布的各版语法规则的交换应使用下列语法版本号以便彼此区别。

ISO 9735:1988——语法版本号:1

ISO 9735:1988(1990 年修订并重印版)——语法版本号:2

ISO 9735:1988(1990 年修订并重印版)及其 1992 年第 1 号修订单——语法版本号:3

ISO/IEC 9735 在《联合国用于行政、商业和运输性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)

将来还有可能增加新的部分。

在本标准中,附录 A 和附录 B 是标准的附录,附录 C 到附录 H 是提示的附录。

引　言

根据批式处理的需求，本标准包含了用于在开放环境中交换的电子报文中的数据结构化的应用级规则。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 的一个新增部分。它提供了一种可供选择的管理安全密钥和证书的能力。

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9部分:安全密钥和证书管理报文(报文类型为KEYMAN)

GB/T 14805.9—2001
idt ISO 9735-9:1999

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)

1 范围

本标准规定了批式EDIFACT安全所需的安全密钥和证书管理报文。

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括一个说明,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。

如果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,则这些设备处于一致性状态。

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

当在本标准中标识出相关标准中定义的条文后,这些条文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为本标准的条文。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和IEC的成员维护着当前有效的国际标准的注册。

GB/T 14805.1—1999 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1部分:公用的语法规则及语法服务目录(idt ISO 9735-1:1998)

GB/T 14805.2—1999 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2部分:批式电子数据交换专用的语法规则(idt ISO 9735-2:1998)

GB/T 14805.5—1999 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)(idt ISO 9735-5:1998)

国家质量技术监督局2001-04-09批准　　2001-10-01实施