ICS 35.240.60
L 70

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

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、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/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。

国家质量技术监督局1999-11-11批准 2000-05-01实施

通过适当的加密算法对报文体、客体、报文/包或单个的报文/包/组进行加密，并连同任意安全头段组和安全尾段组一起来提供 EDIFACT 结构(报文、包、段组或交换)的保密性。该加密数据可能被过滤，以便在限定能力的通信网中使用。

5.1.1 批式 EDI 的保密性

5.1.1.1 交换的保密性

图 1 表示了一个通过保密性进行安全处理的交换的结构。服务串通知(UNA)、交换头段(UNB)和交换尾段(UNZ)不受加密的影响。如果使用压缩技术，应在加密前使用。

要在安全头段组中规定加密算法、压缩算法和过滤算法及相关参数。

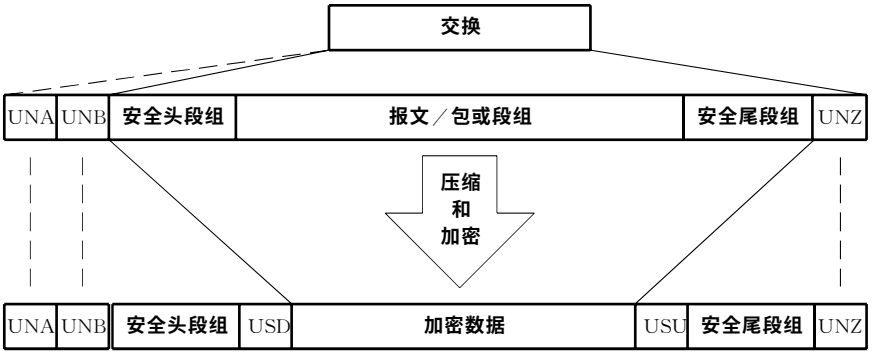

图 1 内容(报文/包或组)已被加密的一个交换的结构(示意图)

5.1.1.2 组的保密性

图 2 表示了一个包含有一个加密组的交换的结构，对于其他的安全服务这个加密组已经过安全处理。组头(UNG)和组尾(UNE)不受加密的影响。

如果使用压缩技术，应在加密前使用。

要在安全头段组中规定加密算法、压缩算法和过滤算法及相关参数。

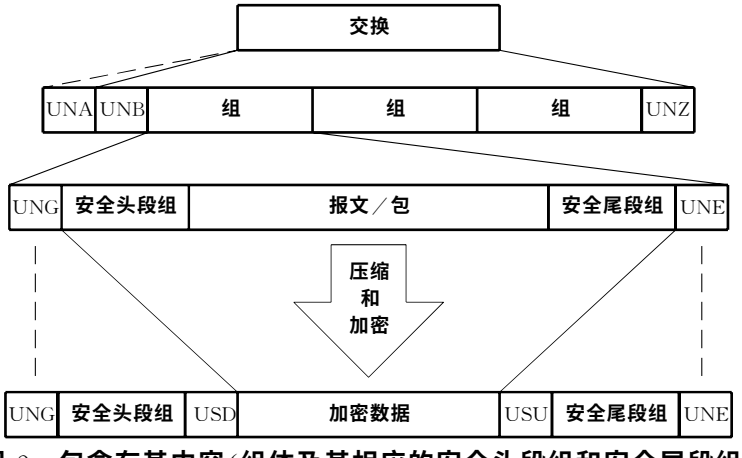

图 2 包含有其内容(组体及其相应的安全头段组和安全尾段组)已被加密的一个组的一个交换的结构

5.1.1.3 报文的保密性

图 3 表示了一个包含有一个加密报文的交换的结构，对于其他的安全服务该加密报文已经过安全处理。报文头段(UNH)和报文尾段(UNT)不受加密的影响。

如果使用压缩技术，应在加密前使用。

要在安全头段组中规定加密算法、压缩算法和过滤算法及相关参数。

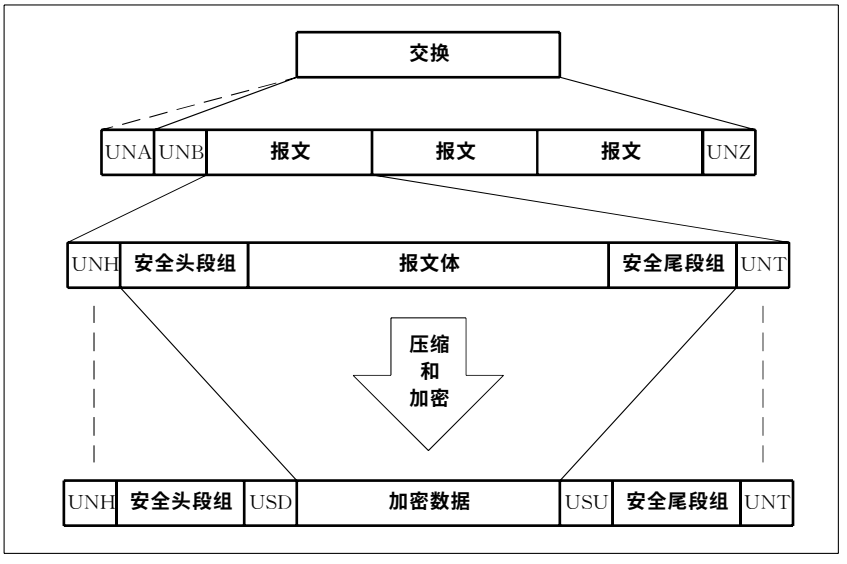

图 3　包含有其内容(报文体及其相应的安全头段组和安全尾段组)已被加密的一个报文的一个交换的结构(示意图)

5.1.1.4　包的保密性

图 4 表示了一个包含有一个加密包的交换的结构,对于其他安全服务该加密包已经过安全处理。包头段(UNO)和包尾段(UNP)不受加密的影响。

如果使用压缩技术,应在加密前使用。

要在安全头段组中规定加密算法、压缩算法和过滤算法及相关参数。

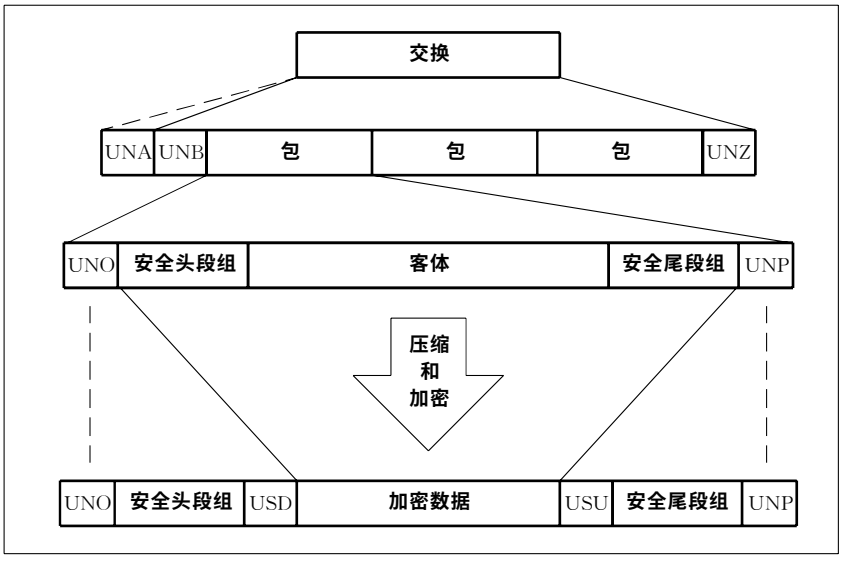

图 4　包含有其内容(客体及其相应的安全头段组和安全尾段组)已被加密的一个包的一个交换的结构(示意图)

5.1.2　数据加密头段和尾段的结构(见图 5)

标记	名称	状态	最大次数
	段组 1	C	99
USH	安全头	M	1
USA	安全算法	C	3
	段组 2	C	2
USC	证书	M	1
USA	安全算法	C	3
USR	安全结果	C	1
USD	数据加密头	M	1
	加密数据		
USU	数据加密尾	M	1
	段组 n	C	99
UST	安全尾	M	1
USR	安全结果	C	1

图 5 安全头段组和安全尾段组的段表

注：USH、USA、USC、USR 和 UST 段在 GB/T 14805.5 中进行了规定。在本部分中，对它们不做进一步说明。

5.1.3 数据段说明

段组 1：USH-USA-SG2（安全头段组）

本段组标识了所采用的安全服务和安全机制，并包含了执行确认计算所需的数据。这里只应含有一个用于保密性的安全头段组。

USH，安全头

本段规定了应用于包括本段在内的 EDIFACT 结构的保密性安全服务（见 GB/T 14805.5 中的定义）。

USA，安全算法

本段标识了安全算法及该算法的用法，并且包含了所需的技术参数。该算法应是应用于报文体、客体、报文/包或报文/包/组的算法。这些算法应是持有者对称算法、持有者压缩算法或持有者压缩完整性算法。

非对称算法不应直接在段组 1 中的 USA 段内引用，只可在 USC 段触发的段组 2 中出现。

如果在加密之前对数据进行压缩，USA 则用于规定算法和可选的操作方式。附加的参数（如初始目录树）可规定为 USA 段中的参数值。

如果采用压缩且所采用的压缩算法不包含内嵌的完整性验证，则可用 USA 段进行规定。完整性验证值是加密前通过压缩的文本计算得到的。在压缩数据内，完整性验证值的位置（即 8 位位组偏移值）可规定为参数值。完整性验证值的大小（以 8 位位组为单位）则通过所采用的完整性验证算法间接地给出。

段组 2：USC-USA-USR（证书段组）

当使用非对称算法时，本段组包含了用来验证应用于 EDIFACT 结构的安全方法所需的数据（见 GB/T 14805.5 的定义）。

USC,证书 14805

本段包含证书拥有者的凭证,并标识生成该证书的认证机构(见 GB/T 14805.5 中的定义)。

USA,安全算法

本段标识了安全算法及该算法的用法,并且包含了所需的技术参数。(见 GB/T 14805.5 中的定义)。

USR,安全结果

本段包含认证机构应用于证书的安全功能的结果(见 GB/T 14805.5 中的定义)。

USD,数据加密头

本段规定了压缩(任选)、加密和过滤(任选)数据的 8 位位组大小。可以规定用于标识所加密的 EDIFACT 结构的参考号。如果给出参考号,USD 和 USU 段中应采用相同的参考号。

若加密前使用填充,则要说明填充的 8 位位组数。

加密数据

本部分包含了采用安全头段组所规定的加密算法和机制进行加密处理后的加密数据。

USU,数据加密尾

本段规定了压缩(任选)、加密和过滤(任选)数据的 8 位位组大小。可以规定用于标识所加密的 EDIFACT 结构的参考号。如果给出了参考号,则 USD 和 USU 段中应采用相同的参考号。

段组 n:UST-USR(安全尾段组)

本段组包含了与安全头段组的链接和应用于 EDIFACT 结构安全功能的结果(见 GB/T 14805.5 的定义)。

UST,安全尾

本段在安全头段组与安全尾段组间建立一个链接,并且说明了包含在这些组中安全段的数目(含 USD 段和 USU 段)(见 GB/T 14805.5 中的定义)。

USR,安全结果

本段包含了应用于 EDIFACT 结构的安全功能的结果,这些安全功能是在被链接的安全头段组中进行规定的(见 GB/T 14805.5 中的定义)。对于保密性的安全服务本段不应出现。

5.1.4 用于保密性的数据加密头段和数据加密尾段

加密成加密数据的 EDIFACT 结构封装在数据加密头段和数据加密尾段内。加密的数据及其相关的安全头段组及安全尾段组将替换原有的报文体、客体或报文/包/组。所采用的加密措施不影响加密的 EDIFACT 结构头和尾。

加密的数据应紧跟在结束 USD 段的分隔符后面,USD 段应以 8 位位组为单位来规定加密数据的长度。USU 段跟随在加密数据之后,USU 段再一次以 8 位位组为单位规定加密数据的长度,其长度应与 USD 段中的相同。

5.1.5 用于保密性的安全头段组和安全尾段组

按 GB/T 14805.5 的定义,应包含一个规定保密性的安全头段组及一个相应的安全尾段组。

用于保密性的安全尾段组应只包括一个 UST 段。

一旦 EDIFACT 结构被加密,就不应对该结构提供其他 EDIFACT 安全服务。

5.2 使用的原则

5.2.1 多种安全服务

如果除了保密性以外还需要多于一种的安全服务，应当根据 GB/T 14805.5 确定的原则，EDIFACT 结构的发送方应在加密之前实施其他的安全服务，接收方则应在解密之后进行相关的验证处理。

5.2.2 保密性

EDIFACT 结构的保密性应按 ISO 10181-5 所规定的原则进行处理。

应在安全头段组中规定保密性的安全服务，而相关的算法应在段组 1 的 USA 段中进行标识。该 USA 段也可包括建立安全的发送方与安全的接收方之间密钥联络所需的数据。

安全发起方应从 EDIFACT 结构头段(交换、组、报文或包)的段终止符后开始对该结构加密，直到该结构段尾(交换、组、报文或包)的第一个字符前止，其结果看做加密的数据。当接收加密的数据时，安全接收方应对加密的数据解密并将其还原为不包括头段和尾段的原始 EDIFACT 结构。

5.2.3 内部表示和过滤函数

加密处理的结果是一个近似随机的位串。这可能会在某些限定能力通信网中产生问题。为了避免这类问题，可采用过滤函数将位串可逆地映射为某个特定的字符集。

采用过滤函数的结果是增加了加密数据的长度。不同的过滤函数可采用不同的扩展因子。有些过滤函数允许过滤后的文本包含目标字符集中的任意字符，其中包括如段终止符的服务字符，而其他过滤函数可能过滤掉这些服务字符。

在 USD 段和 USU 段中数据元“8 位位组数据长度”内传输的数据长度应表示(压缩、)加密(和过滤)数据的长度。该数据将用来决定加密的数据结束。所采用的过滤函数应在保密性安全头段组中 USH 段的 0505(过滤函数，代码型)内指明。

5.2.4 加密前采用压缩技术

加密计算的开销与加密的数据大小有关，因此加密前对数据进行压缩是很有效的。

大多数压缩技术不会影响加密的文本，甚至过滤的文本，如需要压缩应在加密前进行。

因此，当压缩技术应用于保密性安全服务时，安全头段组可以包括加密前数据已被压缩的标识，还可标识所采用的压缩算法和可选参数。在这种情况下，当对加密数据进行解密后，应在恢复原始 EDIFACT 结构前对数据进行解压。

5.2.5 操作的处理次序

5.2.5.1 加密及相关的操作

当对 EDIFACT 结构实施保密性安全处理时，应执行如下操作：

a) 压缩 EDIFACT 结构(任选)并根据压缩数据计算完整性值(任选)；

b) 加密(已压缩和完整性保护的)EDIFACT 结构；

c) 过滤(已压缩和完整性保护的)加密数据(任选)。

5.2.5.2 解密和相关操作

当将加密的 EDIFACT 结构还原为原有的 EDIFACT 结构时，应执行如下操作：

a) 对已过滤的加密数据消过滤(如已过滤)；

b) 对加密数据解密；

c) 验证压缩数据的完整性值(如果存在完整性值)并扩展(即解压)已解密数据以还原为原始 EDIFACT 结构(如果被压缩)。

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）

A1 段目录

A1.1 段目录规范说明

功能 段的功能。

位置 段表中的独立数据元或复合数据元的顺序位置号。

标记 段目录中的所有服务段的标记以字母“U”开头。所有服务复合数据元的标记以字母“S”开头，所有服务简单数据元的标记以数字“0”开头。

名称 复合数据元的英文名称用大写字母表示。
独立数据元的英文名称用大写字母表示。
成分数据元的英文名称用小写字母表示。

状态 段中的独立数据元或复合数据元的状态（M 表示必备型，C 表示条件型），或复合数据元中的成分数据元的状态。

最大次数 独立数据元或成分数据元在段中出现的最大次数。

表示 复合数据元中的独立数据元或成分数据元的数据值表示：

a	字母字符；
n	数字字符；
an	字母数字字符；
a3	3 位字母字符，定长；
n3	3 位数字字符，定长；
an3	3 位字母数字字符，定长；
a..3	最多为 3 位字母字符；
n..3	最多为 3 位数字字符；
an..3	最多为 3 位字母数字字符。

A1.2 从属注释标识符

代码	名 称
D1	有一项且仅有一项
D2	全有或全无
D3	有一项或多项
D4	有一项或无
D5	如果第一项有，则全有
D6	如果第一项有，则至少有一项
D7	如果第一项有，则其他项全无

从属注释标识的定义，参看 GB/T 14805.1—1999 中的 11.5。

A1.3 按标记排列的段索引

标记	名称
USD	数据加密头（Data encryption header）
USU	数据加密尾（Data encryption trailer）

A1.4 按英文名称排列的段索引

标记	名称
USD	数据加密头(Data encryption header)
USU	数据加密尾(Data encryption trailer)

A1.5 段的说明

注：在此只包含 GB/T 14805 其他部分未被定义的段。

USD 数据加密头

功能：规定了紧随本段段终止符后的加密数据大小(即 8 位位组数据的长度)。

位置	标记	名称	状态	最大次数	表示	注
010	0556	8 位位组数据的长度	M	1	n..18	
020	0518	加密参考号	C	1	an..35	
030	0582	填充位组数	C	1	n..2	

USU 数据加密尾

功能：提供加密数据的结尾。

位置	标记	名称	状态	最大次数	表示	注
010	0556	8 位位组数据的长度	M	1	n..18	1
020	0518	加密参考号	C	1	an..35	2

注

1 0556，该值应和相应的 USD 段中 0556 值相同。

2 0518，该值应和相应的 USD 段中 0518 值相同。

A2 简单数据单元的目录

A2.1 简单数据元规范说明

简单数据元目录中的所有服务简单数据元的标记以数字“0”开头。

名称 简单数据元的名称。

描述 简单数据元的描述。

表示 简单数据元的数据值表示：

a	字母字符；
n	数字字符；
an	字母数字字符；
a3	3 位字母字符，定长；
n3	3 位数字字符，定长；
an3	3 位字母数字字符，定长；
a..3	最多为 3 位字母字符；
n..3	最多为 3 位数字字符；
an..3	最多为 3 位字母数字字符。

A2.2 按标记排列的简单数据元索引

标志	名称
0518	加密参考号(Encryption reference number)
0556	8 位位组的数据长度(Length of data in octets of bits)

0582 **填充位组数**(Number of padding bytes)

A2.3 **按英文名称排列的简单数据元索引**

标记 名称

0518 **加密参考号**(Encryption reference number)

556 **8 位位组的数据长度**(Length of data in octets of bits)

0582 **填充位组数**(Number of padding bytes)

A2.4 **简单数据元的说明**

注：在此只有包含 GB/T 14805 其他部分未定义的简单数据元。

0518 **加密参考号**

描述：加密的 EDIFACT 结构的参考号。

表示：an..35

0556 **8 位位组的数据长度**

描述：8 位位组的数据的计数。

表示：an..18

0582 **填充位组数**

描述：填充位组数。

表示：n..2

附 录 B
(提示的附录)
报文保护示例

在此提供一个示例来解释安全服务段的应用。

这个报文保密性的示例是基于假定的 EDIFACT 付款通知。这里描述的安全机制完全与报文类型无关并且可以应用于任何 EDIFACT 报文。

本示例说明了当一个基于对称算法的方法被应用时，如何使用安全服务段来提供报文内容的保密性。伙伴间事前已交换秘密密钥，并且安全头段组只包含两个相当简单的段。

B1 概述

1995 年 4 月 9 日，A 公司委托 A 银行(分类代码 603000)，记入 A 公司借方帐号 00387806 款值 54345.10 英镑。此款项要付给 B 银行(分类代码 201827)中 West Dock，Milford Haven 的 B 公司的帐号 00663151。付款以支票 62345 结算。收款人是销售部的 Jones 先生。

A 银行要求采用“报文保密性”的安全服务功能来对该付款通知进行加密处理。

这种要求是通过报文发送端采用对称“数据加密标准”(DES)对报文体进行加密来实现的。假定在 A 公司和 A 银行间秘密 DES 密钥已被事先交换。为降低信息传输量，在应用加密技术前对报文体进行压缩。用于压缩报文体的算法是 ISO 12042。

B2 安全细目

以下将列出与保密性有关的安全头段组和安全尾段组。

安全头	
安全服务	报文保密性
安全参考号	该安全头的参考号是 1
过滤函数	用十六进制过滤器过滤全部二进制值
源字符集编码	当加密时报文以在 GB/T 1988—1998《信息技术　信息交换用七位编码字符集》(即 ASCII 码)8 位进行编码
安全标识细目 报文发送方(加密报文的用户)	 A 公司的 Smith 先生
安全标识细目 报文接收方者(解密报文的用户)	 A 银行
安全序号	该报文的安全序号是 001
安全日期和时间	安全时间标记是:日期:1995 04 09 时间:13:59:50
安全算法	
安全算法 算法的使用 密钥算法的操作方式 填充算法	为实现报文保密性所使用的对称算法 使用密码块链接方式 使用 EDS 算法 填充方式采用二进制零
算法参数 算法参数限定符 算法参数值	 为预先交换对称密钥的名称,标识算法参数值 采用称为 ENC-KEY1 的密钥
安全算法	
安全算法 算法的使用 算法	 加密之前为缩小报文量采用压缩算法 采用 ISO 12042 压缩算法
加密头	
8 位位组数据长度 加密参考号 填充位组数	压缩、加密和过滤报文体的大小 参考号是 1 填充位组数是 4
加密数据	
加密数据	压缩,加密和过滤报文体
加密尾	
8 位位组数据长度 加密参考号	压缩、加密和过滤报文体的大小 参考号是 1
安全尾	
安全段数 安全参考号	值为 6(即 USH,USA,USA,USD,USU,UST) 安全尾的参考号是 1

附 录 C
（提示的附录）
处 理 示 例

C1 加密示例

图 C1 是一个处理示例，执行可选择不同的次序和不同的部分实现。

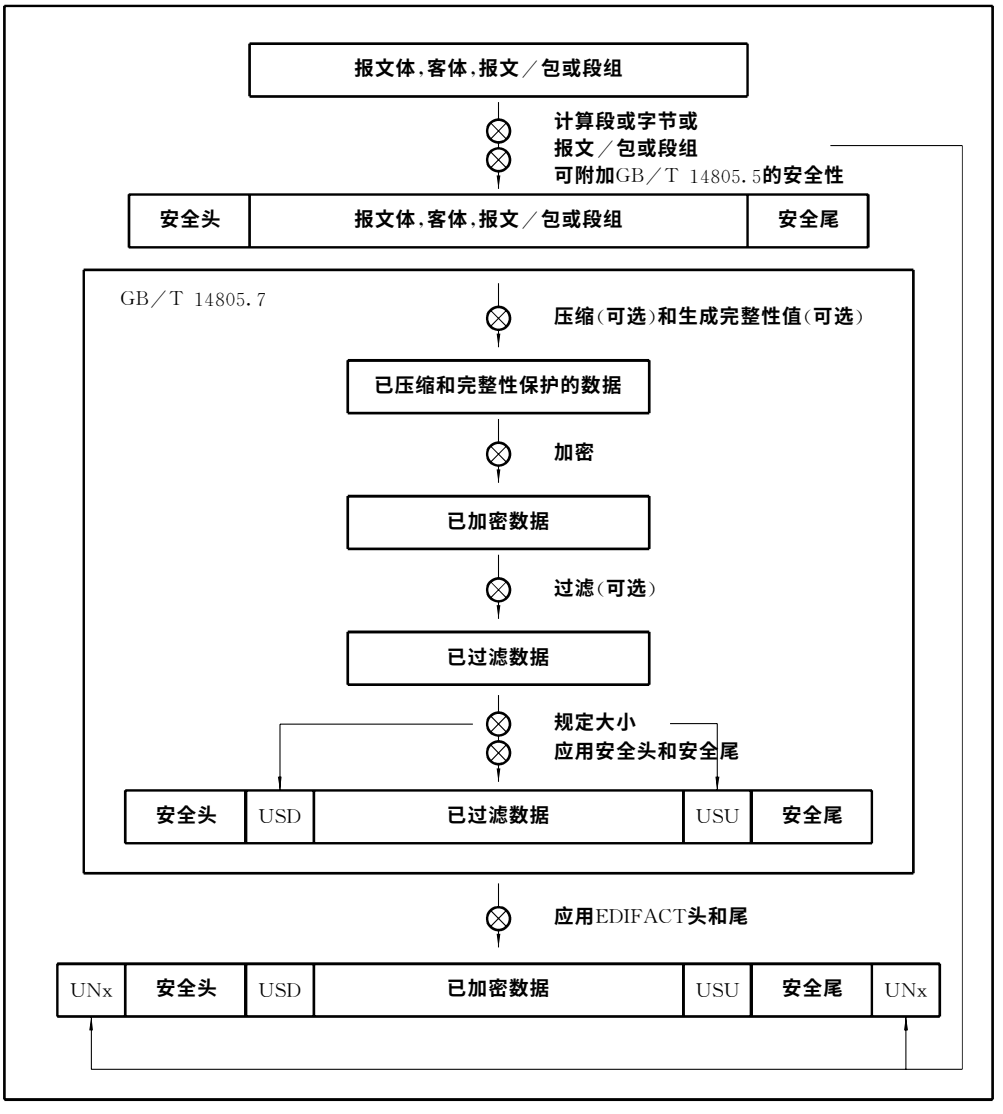

图 C1 加密 EDIFACT 结构所涉及的处理过程

C2 解密示例

图 C2 是一个处理示例。执行可选择不同的次序和不同的部分实现。

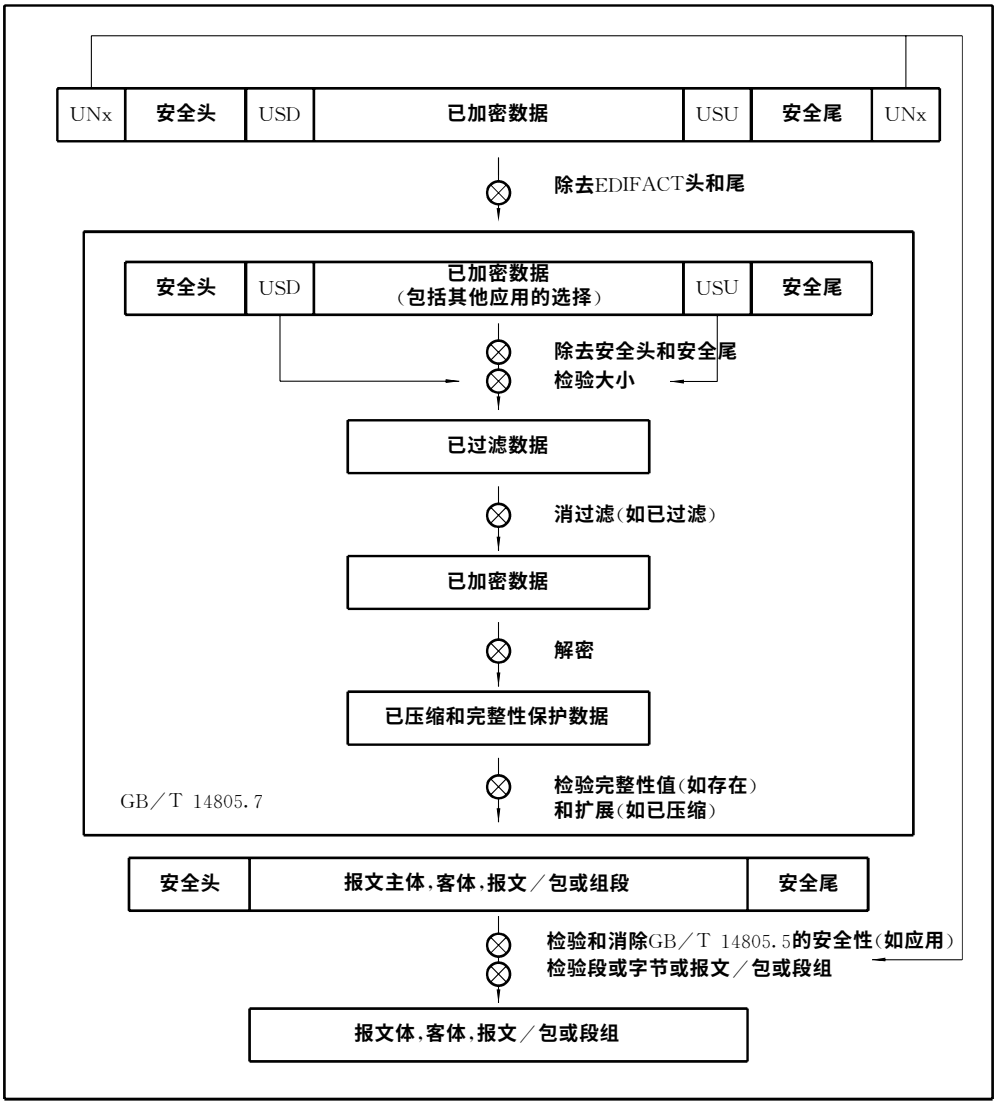

图 C2　解密 EDIFACT 结构所涉及的处理过程

附　录　D
（提示的附录）
保密性服务和算法

D1　目的和范围

本附录给出了安全段组中数据元和代码值可能组合的几种示例。所选择的这些示例是用来说明几种基于国际标准而被广泛应用的安全技术。

由于可组合的全集太大，因此本附录不能全部列出。在此所做的选择不必认为是对该算法或操作方式的认可。用户可以根据所要防范的安全威胁选择合适的安全技术。

本附录的目的是一旦用户选定了安全技术，便向他提供一个全面的起点以得到适合其特定应用的解决方案。

矩阵中使用的代码表（完整代码表的子集）

0501	**安全服务,代码型**
4	**保密性**
0525	**加密的操作方式,代码型**
2	CBC(DES **操作方式**)
16	DSMR(**给报文复原的数字签名模式**)
18	CBC-TBSS(**具有** TBSS **填充的** DES **操作方式**)
19	RSA-TBSS(**采用具有** TBSS **填充方式的** RSA **进行封装**)
36	CTS(RC5 **操作方式**)
0531	**算法参数限定符**
5	**对称密钥,以对称密钥加密**
6	**对称密钥,以公开密钥加密**
9	**对称密钥名称**
10	**密钥加密密钥名称**
12	**模数**
13	**指数**
14	**模数长度**
0577	**安全参与方限定符**
1	**报文发送方**
2	**报文接收方**
3	**证书持有者**
4	**鉴别方**

0523	**算法的使用,代码型**
3	**发布者签名**
4	**发布者散列**
5	**持有者加密**
8	**持有者压缩**
9	**持有者压缩完整性**
0527	**算法,代码型**
1	DES(**数据加密标准**)
4	IDEA(**国际数据加密算法**)
10	RSA
14	RIPEMD-160(**专用的散列函数**#1)
18	ZLIB(**数据压缩算法**)
25	CRC-32(**循环冗余校验**)
27	ISO 12042(**数据压缩**)
29	RC5(**可变密钥大小对称分组密码**)
0563	**确认值限定符**
1	**唯一确认值**
0589	**填充算法,代码型**
1	**零填充**
2	PKCS#1 **填充**
4	TBSS **填充**

使用的缩略语

a123,1,ABC99	=	**安全参考号的表示法**
CA	=	**认证机构**
CA-Sig	=	**认证机构签名**
Enc-Key	=	**加密密钥**
Exp	=	**公开指数**
KEK-N	=	**密钥加密密钥**
Key-N	=	**密钥名称**
Len	=	**(已压缩)、已加密(和过滤)的** 8 **位位组数据长度**
Mod	=	**公开模数**
Mod-L	=	**公开模数长度**
PK/CA	=	**认证机构的公开密钥**

D2 采用对称算法和集成式安全段的组合来实现对 EDIFACT 结构的保密性

表 D1 为下列特定情况建立了的关系：

——集成式报文/包/组/交换级的安全(GB/T 14805.7)。

——使用对称算法进行加密。

——使用对称算法和非对称算法进行密钥交换。

——提供的安全服务是保密性。

——使用 DES、IDEA 和 RC5 算法来提供保密性。这里给出 3 个示例：

1) DES、CBC 操作方式及接收方所知的秘密密钥。所需的秘密密钥是通过发送方和接收方共享的“密钥加密密钥”加密的。“密钥加密密钥”是通过该密钥名称来引用的。本算法不使用数据压缩技术。填充方式采用零填充并需要有关填充位组数的附加信息。

2) RC5、CTS 操作方式及接收方所知的秘密密钥。所需的秘密密钥是通过发送方和接收方共享的“密钥加密密钥”加密的。“密钥加密密钥”是通过该密钥名称来引用的。加密前，应用 ISO 12042 压缩技术。

3) IDEA、CBC 操作方式及 TBSS 填充技术。用于加密的秘密密钥是通过使用接收方的公开密钥进行交换的。公开密钥是嵌入在证书中的。加密前，应用 Z-lib 压缩和 CRC—32 完整性保护技术。

——虽然发送方和接收方共享密钥，但双方事先未就加密机制完全达成协议。因此，所用的全部算法和操作方式都要明确指出。

——这里只列出与实际应用的安全技术、算法及操作方式相关的安全区域。

——USC 段包含了认证机构用于签发证书的散列函数标识和签名函数。接收方已知道认证机构用于证书签名的公开密钥。该公开密钥在 USC 段中通过名称被引用。

表 D1 阵矩关系

标 记	名 称	状态	最大次数	保密性例 1	保密性例 2	保密性例 3	注
SG 1		C	99	每个安全服务 1 个			1
USH	安全头	M	1				
0501	安全服务，代码型	M		4	4	4	
0534	安全参考号	M		a123	1	ABC99	
S500	安全标识细目	C	2	（发送方）			
0577	安全参与方限定	M		1	1	1	
0511	安全参与方标识	C		发送方标识	发送方标识	发送方标识	
S500	安全标识细目	C	2	（接收方）			
0577	安全参与方限定	M		2	2	2	
0511	安全参与方标识	C		接收方标识	接收方标识	接收方标识	
USA	安全算法	C	3	（加密算法）			
S502	安全算法	M	1				
0523	算法的使用，代码型	M		5	5	5	
0525	加密的操作方式，代码型	C		2	36	18	
0527	算法，代码型	C		1	29	4	

表 D1 （续）

标　记	名　　称	状态	最大次数	保密性 例 1	保密性 例 2	保密性 例 3	注
0589	填充算法,代码型	C		1	2	4	2
S503	算法参数	C	9	一个加密密钥			
0531	算法参数限定符	M		5	5	6	
0554	算法参数值	M		密钥	密钥	密钥	
S503	算法参数	C	9	一个密钥加密密钥			
0531	算法参数限定符	M		10	10	—	
0554	算法参数值	M		Key-N	Key-N	—	
USA	安全算法	C	3	（压缩算法）			
S502	安全算法	M	1				
0523	算法的使用,代码型	M		—	8	8	
0525	加密的操作方式,代码型	C		—	—	—	
0527	算法,代码型	C		—	27	18	
USA	安全算法	C	3	（压缩完整性算法）			
S502	安全算法	M	1				
0523	算法的使用,代码型	M		—	—	9	
0525	加密的操作方式,代码型	C		—	—	—	
0527	算法,代码型	C		—	—	25	
SG 2		C	2	仅一个:接收方证书			
USC	证书	M	1				
S500	安全标识细目	C	2	（证书持有者）			
0577	安全参与方限定符	M		—	—	3	
0511	安全参与方标识	C		—	—	持有者标记	
S500	安全标识细目	C	2	（鉴别参与方）			
0577	安全参与方限定符	M		—	—	4	
0538	密钥名称	C		—	—	（PK/C 名称）	
0511	安全参与方标识	C		—	—	认证机构标识	
USA	安全算法	C	3	（证书签名认证机构的散列函数）			
S502	安全算法	M	1				
0523	算法的使用,代码型	M		—	—	4	
0525	加密的操作方式,代码型	C		—	—	—	
0527	算法,代码型	C		—	—	14	
USA	安全算法	C	3	（证书签名认证机构的签名函数）			
S502	安全算法	M	1				

表 D1 （续）

标 记	名 称	状态	最大次数	保密性 例 1	保密性 例 2	保密性 例 3	注
0523	算法的使用,代码型	M		—	—	3	
0525	加密的操作方式,代码型	C		—	—	16	
0527	算法,代码型	C		—	—	10	
S503	算法参数	C	9	（认证机构公开密钥指数）			
0531	算法参数限定符	M		—	—	12	
0554	算法参数值	M		—	—	Mod	
S503	算法参数	C	9	（认证机构公开密钥指数）			
0531	算法参数限定符	M		—	—	13	
0554	算法参数值	M		—	—	Exp	
S503	算法参数	C	9	（认证机构公开密钥模数长度）			
0531	算法参数限定符	M		—	—	14	
0554	算法参数值	M		—	—	Mod-L	
USA	安全算法	C	3	（证书持有者的加密函数）			
S502	安全算法	M	1				
0523	算法的使用,代码型	M		—	—	5	
0525	加密的操作方式,代码型	C		—	—	19	
0527	算法,代码型	C		—	—	10	
S503	算法参数	C	9	（持有者公开密钥模数）			
0554	算法参数值	M		—	—	Mod	
S503	算法参数	C	9	（持有者公开密钥指数）			
0531	算法参数限定符	M		—	—	13	
0554	算法参数值	M		—	—	Exp	
S503	算法参数	C	9	（持有者公开密钥模数长度）			
0531	算法参数限定符	M		—	—	14	
0554	算法参数值	M		—	—	Mod-L	
USR	安全结果	C	1				
S508	确认结果	M	2				
0563	确认值限定符	M		—	—	1	
0560	确认值	C		—	—	CA-Sig	
USD	数据加密头	M	1				
0556	8 位位组数据长度	M	1	Len	Len	Len	
0518	加密参考号	C	1	—	A	—	
0582	填充位组数	C	1	3	—	—	3

表 D1 （完）

标 记	名 称	状态	最大次数	保密性 例 1	保密性 例 2	保密性 例 3	注
安全化的数据结构(报文体,客体,报文/包/段组)							
USU	加密数据尾	M	1				
0556	8 位位组数据长度	M	1				
0518	加密参考号	C	1	—	A	—	
SG n		C	99	每个安全服务一个			1
UST	安全尾	M	1				
0534	安全参考号	M		a123	1	ABC99	
0588	安全段数	M	1	5	6	12	

注

1 这两个结构必须有相同出现数。

2 填充仅应用于规定加密算法的 USA 段。

3 填充位组数仅作为示例。

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
*
中国标准出版社出版
北京复兴门外三里河北街16号
邮政编码:100045
电 话:68522112
中国标准出版社秦皇岛印刷厂印刷
新华书店北京发行所发行 各地新华书店经售

*
开本 880×1230 1/16 印张 1½ 字数 39 千字
2000年6月第一版 2000年6月第一次印刷
印数 1—1 000
*
书号:155066·1-16677 定价 14.00 元
*
标 目 408—23

GB/T 14805.7-1999