ICS 35.240.60
L 70

中华人民共和国国家标准

GB/T 14805.5—1999
idt ISO 9735-5:1998

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）

Electronic data interchange for administration, commerce and transport (EDIFACT)—Application level syntax rules (Syntax version number:4)—Part 5:Security rules for batch EDI (authenticity, integrity and non-repudiation of origin)

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 9735-5:1998《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 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)》。

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.×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。

本标准的附录 A、附录 B 是标准的附录,附录 C、附录 D、附录 E、附录 F、附录 G、附录 H 是提示的附录。

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:中国标准化与信息分类编码研究所、电子工业部标准化研究所。

本标准主要起草人:李颖、吴志刚、胡涵景、张荣静、王颜尊、魏宏、刘碧松。

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、商业和运输业电子数据交换的应用级语法规则》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。

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。

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 的一个新增部分。它提供了一种保护批式 EDIFACT 结构(即报文、包、组或交换)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）

GB/T 14805.5—1999
idt ISO 9735-5:1998

Electronic data interchange for administration, commerce and transport (EDIFACT)—Application level syntax rules(Syntax version number:4)—Part 5:Security rules for batch EDI (authenticity, integrity and non-repudiation of origin)

1 范围

本标准规定了用于EDIFACT安全的语法规则。本标准阐述了根据所建立的安全机制为报文/包级、组级和交换级安全提供真实性、完整性和源抗抵赖性的方法。

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 14805.8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。

GB/T 7408—1994 数据元和交换格式 信息交换 日期和时间表示法(eqv ISO 8601:1988)

GB/T 9387.2—1995 信息处理系统 开放系统互连 基本参考模型 第2部分：安全体系结构(idt ISO 7498-2:1989)

GB 13000-1:1993 信息技术 通用多八位编码字符集(UCS) 第1部分：体系结构与基本多文种平面(idt ISO/IEC 10646-1:1993)

GB/T 16264.8—1996 信息技术 开放系统互连 目录 第8部分：鉴别框架(idt ISO/IEC 9594-8:1990)

国家质量技术监督局1999-11-11批准 2000-05-01实施

GB/T 17901.1—1999 信息技术 安全技术 密钥管理 第1部分:框架
ISO/IEC 10181-1:1996 信息技术 开放系统互连 开放系统的安全框架 第1部分:概述
ISO/IEC 10181-2:1996 信息技术 开放系统互连 开放系统的安全框架 第2部分:鉴别框架
ISO/IEC 10181-4:1996 信息技术 开放系统互连 开放系统的安全框架 第4部分:抗抵赖性框架
ISO/IEC 10181-6:1997 信息技术 开放系统互连 开放系统的安全框架 第6部分:完整性框架

4 定义

本标准采用的定义见GB/T 14805.1—1999的附录A。

5 批式EDI的安全头段组和安全尾段组的使用规则

5.1 报文/包级安全——集成报文/包安全

附录C和附录D描述了与报文/包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EDIFACT报文/包级安全的结构。

本标准描述的安全服务,对于任一现有的报文,应通过在UNH段后紧跟安全头段组和在UNT段前加入安全尾段组来提供;对于任一现有的包,应通过在UNO段后紧跟安全头段组和在UNP段前加入安全尾段组来提供。

5.1.1 安全头段组和安全尾段组

图1描述了表示报文级安全的一个交换。

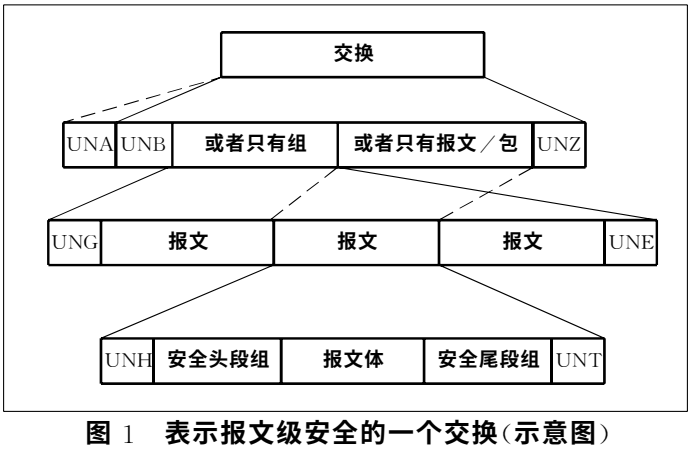

图1 表示报文级安全的一个交换(示意图)

图2描述了表示包级安全的一个交换。

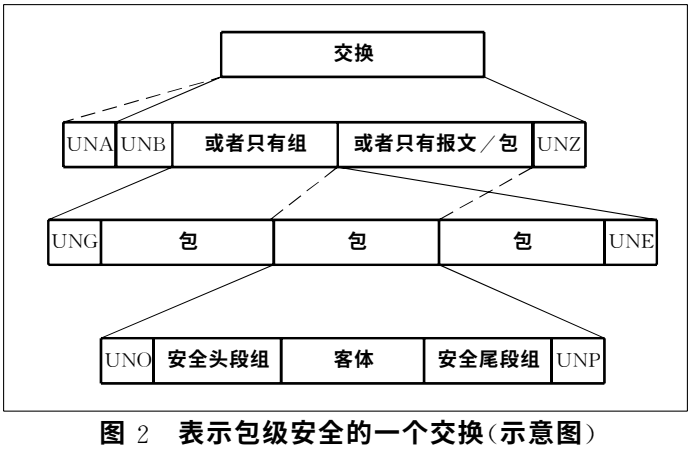

图2 表示包级安全的一个交换(示意图)

5.1.2 安全头段组和安全尾段组的结构(见表 1、表 2)

表 1 安全头段组和安全尾段组的段表(报文级安全)

标记	名称	状态	最大次数
UNH	报文头	M	1
……	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
	报文体		
……	段组 *n* ……	C	99
UST	安全尾	M	1
USR	安全结果	C	1
UNT	报文尾	M	1

表 2 安全头段组和安全尾段组的段表(包级安全)

标记	名称	状态	最大次数
UNO	客体头	M	1
……	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
	客体		
……	段组 *n* ……	C	99
UST	安全尾	M	1
USR	安全结果	C	1
UNP	客体尾	M	1

注:报文头 UNH、报文尾 UNT、客体头 UNO 和客体尾 UNP 在 GB/T 14805.1 中规定,本标准对它们不做进一步说明。

用于安全头段组和安全尾段组的段和数据元的完整目录规范见附录 B。

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。

如果对报文/包采用不同的安全服务(如完整性和源抗抵赖性)或几个参与方采用了相同的安全服务,则在同一报文/包中可以有几个不同的安全头段组。

USH,安全头

本段规定了应用于包含本段在内的报文/包的安全服务。

与该安全服务有关的各参与方(即安全数据元发起方和安全数据元接受方)可在本段中标识,除非

在采用非对称算法时，它们被无歧义地用证书（即 USC 段）标识。

在下述情况之一出现时，应在 USH 段中使用复合数据元安全标识细目（S500）：

——采用对称算法；

——采用非对称算法时为区别安全发起方证书和安全接受方证书而提交两个证书。

在后一种情况下，S500 中的参与方标识（数据元 S500/0511，S500/0513，S500/0515，S500/0568 中的任一个）应与在段组 2 的 USC 段中出现的某个 S500 中被限定为“证书持有者”的参与方标识相同，同时，数据元 S500/0577 应标识所涉及的参与方的功能（即发起方或接受方）。

复合数据元安全标识细目中的数据元密钥名称（S500/0538）可用来在发送方和接收方之间建立密钥关系。

该密钥关系也可通过使用段组 1 的 USA 段中的复合数据元算法参数中的数据元密钥标识（S500/0554）来建立。

如果不需要传送段组 1 中的 USA 段（因为加密机制已事先在参与方间商定），可使用 USH 段中的 S500/0538。

然而，在同一安全头段组中，本标准强烈推荐使用 USH 中的 S500/0538 或 USA 中带有限定符的 S503/0554 中的一个，而不是两个都使用。

USH 段可规定用于段组 1 中 USA 段以及相应的安全尾组中的 USR 段的二进制区的过滤函数。

USH 段可包含一个用于提供顺序完整性的安全顺序号和安全元素的创建日期。

USA，安全算法

本段标识了安全算法及该算法的用法，并包含了所需的技术参数。该算法应是直接应用于报文/包的算法。该算法可以是对称算法、散列函数或压缩算法。例如，对数字签名而言，该算法指明所使用的与报文相关的散列函数。

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

USA 段允许出现三次。一次用于提供 USH 段中规定的安全服务所需的对称算法或散列函数，其余两次在 GB/T 14805.7 中描述。

需要时，可使用填充机制指示。

段组 2：USC-USA-USR（证书组）

当使用非对称算法时，本段组包含了用来验证应用于报文/包的安全方法所需的数据。当采用非对称算法来标识所使用的非对称密钥对时，即使不使用证书，也应使用证书段组。

在 USC 段中，应给出整个证书段组（包括 USR 段）或只用于无歧义地标识所使用的非对称密钥对所需的数据元。如果两个参与方已经交换了证书或如果证书可从数据库中获得，则可避免整个证书的出现。

当决定引用非 EDIFACT 证书（诸如×509）时，应在 USC 段的数据元 0545 中标识该证书的语法和版本。这样的证书可在 EDIFACT 包中传送。

本段组允许出现两次。一次用于报文/包的发送方证书（报文/包的接收方将用它来验证发送方的签名），另一次则是在发送方为了对称密钥的保密性而使用接收方公开密钥的情况下，用于报文/包的接收方证书（只用证书参考引用）。

如果在同一个安全头段组中该段组出现两次，则可用复合数据元安全标识细目（S500）和数据元证书参考（0536）将它们区分开来。

如果不使用非对称算法，该段组应被省略。

USC，证书

本段包含证书持有者的凭证，并标识生成该证书的认证机构。代码型数据元过滤函数(0505)应标识用于段组 2 的 USA 段和 USR 段的二进制区的过滤函数。

USC 段中的 S500 可以出现两次，一次用于证书持有者(识别使用包含于本证书内的公开密钥相对应的私有密钥进行签名的那一方)，另一次用于证书发布者(认证机构——CA)。

USA，安全算法

本段标识了安全算法及该算法用法，并包括所需的技术参数。在段组 2 中，USA 段可出现三次，分别标识：

1 证书发布者用于计算证书的散列值的算法(散列函数)

2 证书发布者用于生成证书(即签署根据证书内容计算出的散列函数的结果)的算法(非对称算法)

3a 发送方用于签署报文/包(即签署根据证书内容计算出的散列函数的结果)的算法(非对称算法)，或

3b 发送方使用的接收方非对称算法(非对称算法)，该算法用来加密应用于报文/包内容的对称算法所需的密钥，并且这个密钥在由 USH 段触发的段组 1 中被引用。

需要时，可使用填充机制指示。

USR，安全结果

本段包含了认证机构应用于证书的安全功能的结果。该结果应是由认证机构通过签署根据凭证数据计算出的散列结果而得出的证书的签名。

对证书而言，签名计算始于 USC 段的第一个字符(即“U”)，终于最后一个 USA 段的最后一个字符(包括紧随该 USA 段的分隔符)。

段组 n：UST-USR(安全尾组)

本段组包含与安全头段组的链接和应用于报文/包的安全功能的结果。

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，并说明了包含在这些组中安全段的数目。

USR，安全结果

本段包含应用于报文/包的安全功能的结果，这些安全功能是在被链接的安全头段组中规定的。根据在被链接的安全头段组中规定的安全机制，该结果应为下列两种结果之一：

——根据在安全头段组的段组 1 中的 USA 段中指明的算法直接对报文/包进行计算而得出的结果。

——通过用非对称算法签署散列结果而计算出来的结果，其中非对称算法在安全头段组的段组 2 中的 USA 段中指明，散列结果是根据在安全头段组的段组 1 中的 USA 段中指明的算法对报文/包进行计算而得出的。

5.1.4 安全应用的范围

安全应用的范围有两种可能性：

a) 每个完整性值、鉴别值及数字签名的计算始于当前的安全头段组，并包含当前的安全头段组和报文体/客体本身。在这种情况下，安全应用的范围不应包括其他的安全头段组或安全尾段组。

安全头段组始于第一个字母“U”，终于结束该安全头段组的分隔符；报文体/客体始于结束最后一个安全头段组的分隔符之后的第一个字符，终于第一个安全尾段组的第一个字符前的分隔符。

因此，以这种方式集成的安全服务的执行顺序未被规定。它们彼此间完全独立。

图 3 描述了上述这种情况（在安全头段组 2 中定义的安全服务的应用范围用阴影框表示）。

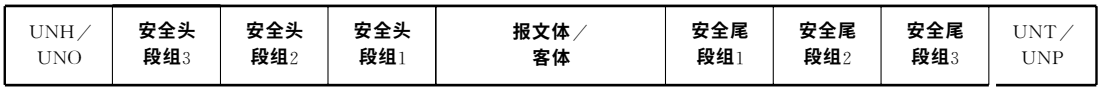

图 3 应用范围：仅为安全头段组和报文体/包（示意图）

b）计算始于当前的安全头段组，并包含当前的安全头段组和有关的安全尾段组。在这种情况下，安全应用的范围应包括当前的安全头段组、报文体/客体以及其他所有被嵌入的安全头段组和安全尾段组。

该范围应包括从当前的安全头段组的第一个字符“U”到有关的安全尾段组的第一个字符之前的分隔符的每一个字符。

图 4 描述了上述这种情况（在安全头段组 2 中定义的安全服务的应用范围用阴影框表示）。

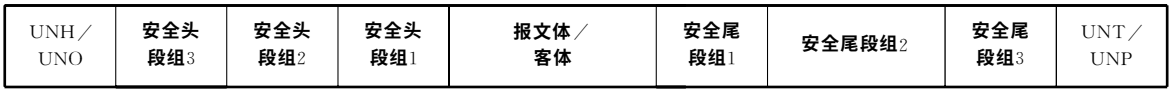

图 4 应用范围：从安全头段组到安全尾段组（示意图）

对每个新增的安全服务，可选择上述两种范围中的一个。

在上述两种情况中，安全头段组和有关的安全尾段组之间的关系应由 USH 和 UST 段中的数据元安全参考号提供。

5.2 使用原理

5.2.1 服务的选择

安全头段组可包含下列通用信息：

——所应用的安全服务；

——有关的参与方的标识；

——所使用的安全机制；

——“唯一的”值（顺序号和/或时间标记）；

——接收的抗抵赖性请求。

当同一 EDIFACT 结构需要多种安全服务时，安全头段组可以出现多次。这就是涉及多对参与方的情况。但是，当同一对参与方需要多个安全服务时，这些服务可以含于一对安全头段组和安全尾段组之中，就好像某个服务隐含于其他服务中一样。

5.2.2 真实性

如果 EDIFACT 结构要求源鉴别服务，则应使用一对适当的安全头段组和安全尾段组并根据 ISO 10181-2 规定的原理提供该项服务。

源鉴别安全服务应在段组 1 的 USH 段中规定，算法则在该段组的 USA 段中标识。

安全发起方应计算在安全尾段组中的 USR 段中传送的真实性值。安全接受方应查证该真实性值。

如果基于防拆硬件或可信第三方实施适当的“源鉴别”服务，则可把它当作一个“源抗抵赖性”服务的实例。这样的作法应在交换协定中予以明确。

5.2.3 完整性

如果 EDIFACT 结构要求内容完整性服务，则应使用一对适当的安全头段组和安全尾段组并根据 ISO 10181-6 规定的原理提供该项服务。

完整性安全服务应在段组 1 的 USH 段中规定，算法则在段组 1 的 USA 段中标识。该算法应是散列函数或对称算法。

安全发起方应计算在安全尾段组中的 USR 段中传送的完整性值。安全接受方应查证该完整性值。

完整性服务可以通过源鉴别服务或源抗抵赖性服务的“副产品”的形式获得。

如果需要顺序完整性服务，则应在安全头段组中或者包含安全顺序号和安全时间标记的两者之一，或者包含这两者；同时还应使用内容完整性服务、源鉴别服务和源抗抵赖性服务中的一个。

5.2.4 源抗抵赖性

如果 EDIFACT 结构要求源抗抵赖性服务，则应使用一对适当的安全头段组和安全尾段组并根据 ISO 10181-4 中规定的原理提供该项服务。

源抗抵赖性安全服务应在段组 1 的 USH 段中规定，散列算法则在段组 1 中的 USA 段中标识，如果使用证书，还应在段组 2 的 USA 段中标识用于签名的非对称算法。

如果证书不在报文/包中传送，接收方应知晓所采用的算法为非对称算法。在这种情况下，该非对称算法应在交换协定中明确。

安全服务发起方应计算在安全尾段组的 USR 中传送的数字签名，安全服务接受方应查证该数字签名值。

源抗抵赖性服务还能提供内容完整性和源鉴别服务。

5.3 符合 EDIFACT 语法的内部表示法和过滤器

采用数学算法计算完整性数值和数字签名带来两个问题：

第一个问题是计算结果依赖于字符集的内部表示。这样，发送方数字签名的计算及接收方对该签名的验证就应使用同一字符集编码来完成。因此，发送方可以指明用于生成原始的安全确认结果的表示法。

第二个问题是安全的计算结果类似随机的位模式。这可能会导致在传输期间和使用翻译软件时出现问题。为避免这些问题，利用过滤函数将位模式可逆地映射到所使用的字符集的特定的表示法上。为简单起见，每个安全服务只使用一个过滤函数。这个映射的结果中所出现的异常终止符通过加入一个转义序列来处理。

6 批式 EDI 的交换和组的安全头段组和安全尾段组的使用规则

6.1 组级和交换级的安全——集成的报文安全

与报文/包传送相关的安全威胁及针对这些威胁的安全服务（见附录 C 和附录 D）也适用于组级和交换级。

在前一章描述的用于报文/包的安全技术，也可用于交换级和组级。

就组级和交换级安全而言，应采用与报文/包级安全中相同的安全头段组和安全尾段组，即使安全应用于多个以上的级上，头尾交叉引用应总是应用于同一级。

在报文/包级应用安全时，被保护的结构是报文体或客体；在组级时，是该组中包括所有报文/包的头和尾在内的所有报文/包的集合；在交换级时，是该交换中包括所有报文/包或组的头和尾在内的所有报文/包或交换的集合。

6.1.1 安全头段组和安全尾段组

图 5 描述了同时含有交换级安全和组级安全的一个交换。

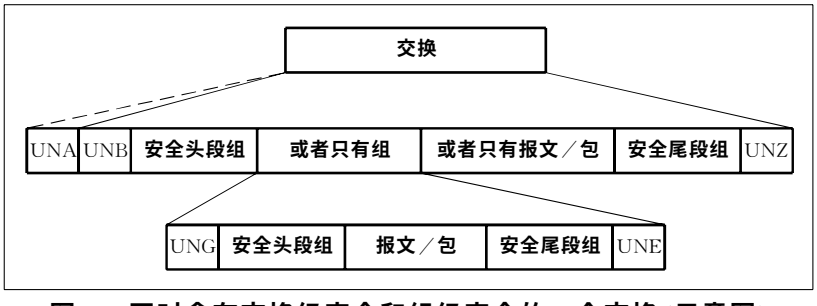

图 5 同时含有交换级安全和组级安全的一个交换（示意图）

6.1.2 安全头段组和安全尾段组的结构（见表 3、表 4）

表 3　安全头段组和安全尾段组段表(仅为交换级安全)

标记	名称	状态	最大次数
UNB	交换头	M	1
……	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
	组或报文/包		
……	段组 *n* ……	C	99
UST	安全尾	M	1
USR	安全结果	C	1
UNZ	交换尾	M	1

表 4　安全头段组和安全尾段组段表(仅为组级安全)

标记	名称	状态	最大次数
UNG	组头	M	1
……	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
	报文/包		
……	段组 *n* ……	C	99
UST	安全尾	M	1
USR	安全结果	C	1
UNE	组尾	M	1

注：交换头 UNB、交换尾 UNZ、组头 UNG 和组尾 UNE 在 GB/T 14805.1 中规定，因而不在本标准中作进一步的描述。

段和数据元的完整目录规范见附录 B。

6.1.3　安全应用的范围

安全应用的范围有两种可能性：

a) 每个完整性值、鉴别值及数字签名的计算始于当前的安全头段组，并包含当前的安全头段组和组/包本身。在这种情况下，安全应用的范围不应包括其他的安全头段组或安全尾段组。

安全头段组始于第一个字母“U”，终于结束该安全头段组的分隔符；组或报文/包始于结束最后一个安全头段组的分隔符之后的第一个字符，终于第一个安全段组的第一个字符前的分隔符。

因此，以这种方式集成的安全服务的执行顺序未被规定。它们彼此间完全独立。

图 6 和图 7 描述了上述这种情况(在安全头段组 2 中定义的安全服务的应用范围用阴影框表示)。

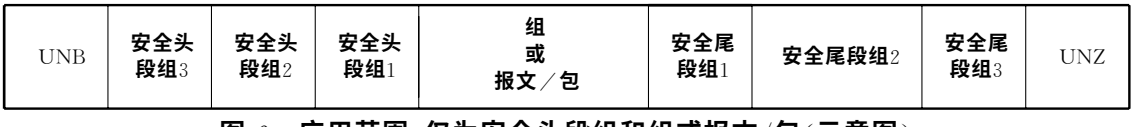

图 6　应用范围：仅为安全头段组和组或报文/包(示意图)

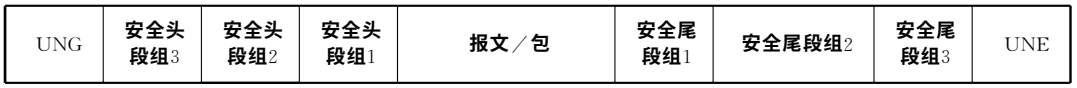

图 7　应用范围：仅为安全头段组和报文/包（示意图）

b）计算始于并包含当前的安全头段组，终于有关的安全尾段组。在这种情况下，安全应用的范围应包括当前的安全头段组、组或报文/包以及其他所有被嵌入的安全头段组和安全尾段组。

该范围应包括从当前的安全头段组的第一个字符“U”到有关的安全尾段组的第一个字符之前的分隔符的每一个字符。

图 8 和图 9 描述了上述这种情况（在安全头段组 2 中定义的安全服务的应用范围用阴影框表示）。

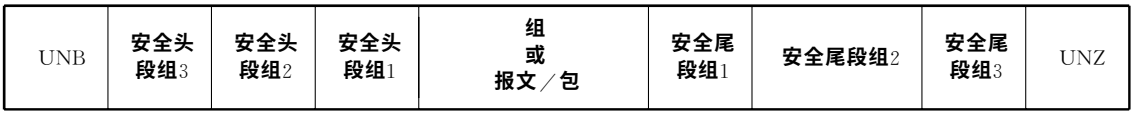

图 8　应用范围：从安全头段组到安全尾段组（示意图）

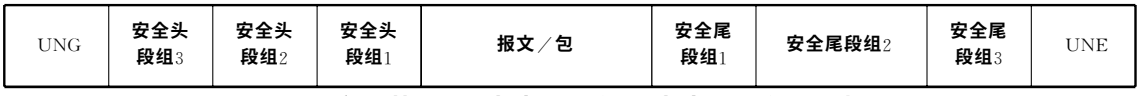

图 9　应用范围：从安全头段组到安全尾段组（示意图）

对每个新增的安全服务，可选择上述两种范围中的一个。

在上述两种情况中，安全头段组和有关的安全尾段组之间的关系应由 USH 和 UST 段中的数据元安全参考号提供。

附 录 A
（标准的附录）
定 义

A1 非对称算法 asymmetric algorithm

一种使用公开密钥和私有密钥的密码算法。

A2 鉴别 authentication

见“数据源鉴别”。

A3 证书 certificate

用户的公开密钥连同其他相关信息，并由认证机构用私有密钥进行签名使其不可伪造。

A4 认证机构 certification authority

受一个或多个用户信任的、负责创建和分发证书的机构。

A5 保密性 confidentiality

信息不泄露给未被授权的个人、实体或进程或不为其所用的特性。

A6 凭证 credential

用于为一个实体建立所声明的身份的数据。

A7 密码学 cryptography

一门包括了对数据进行变换的原理、手段和方法的学科，其目的是隐藏它的数据内容，防止对它进行篡改和/或未被授权地使用。

A8 数据完整性 data integrity

数据没有遭受到以未被授权的方式进行的篡改或破坏的特性。

A9 数据源鉴别 data origin authentication

用于确认接收到的数据的源与所声明的一致。

A10 解密处理 decryption

见“解密”。

A11 解密 decipherment

与一个可逆的加密过程对应的逆过程。

A12 数字签名 digital signature

附加到数据单元上的一些数据或是对数据单元所作的一种密码变换（见“密码学”），这种数据或密码变换允许数据单元的接收方用以确认数据单元的源和数据单元的完整性，并保护数据，以免被人（如

接收方)进行伪造。

A13 加密 encipherment

对数据进行密码变换(见“密码学”)以产生密文。

A14 加密处理 encryption

见“加密”。

A15 过滤 filtering

把含有任意位模式的八位位组转换为语法能支持的字符集的八位位组的过程。

A16 散列函数 hash function

把值从一个大(可能很大)的区域映射到一个小的区域的(数学)函数。一个“好的”散列函数是指该函数的结果应能均匀地(而且随机地)分布在由函数产生的值域中。

A17 完整性 integrity

见“数据完整性”。

A18 密钥 key

控制加密和解密操作的一个符号序列。

A19 抗抵赖性 non-repudiation

在一次通信中涉及的那些实体之一不承认参加了该通信的一部分或全部。

A20 私有密钥 private key

(在公开密钥密码体制中)用户密钥对中只能由该用户知道的那个密钥。

A21 公开密钥 public key

(在公开密钥密码体制中)用户密钥对中为公众所知的那个密钥。

A22 秘密密钥 secret key

用于对称密码技术并只能由一组特定实体使用的密钥。

A23 对称算法 symmetric algorithm

加密和解密或鉴别和确认都采用同一密钥值的一种密码算法。

A24 威胁 threat

一种潜在的对安全的侵害。

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）

B1 段目录

B1.1 段规范说明：

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。

B1.2 从属性注释标识符

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

从属性注释标识符的定义见 GB/T 14805.1—1999 的 11.5。

B1.3 按段标记字母顺序排列的段索引

标记	名 称
USA	安全算法（Security algorithm）
USC	证书（Certificate）
USH	安全头（Security header）

USR	**安全结果**(Security result)	
UST	**安全尾**(Security trailer)	

B1.4 按英文名称的字母顺序排列的段索引

标记	名　　称
USC	**证书**(Certificate)
USA	**安全算法**(Security algorithm)
USH	**安全头**(Security header)
USR	**安全结果**(Security result)
UST	**安全尾**(Security trailer)

B1.5 段规范

USA **安全算法**

功能:标识安全算法及该算法的用法,并包含所需的技术参数。

位置	标记	名称	状态	最大次数	表示	注
010	S502	**安全算法**	M	1		
	0523	**算法的使用,代码型**	M		an..3	
	0525	**密码操作方式,代码型**	C		an..3	
	0533	**操作方式代码表标识符**	C		an..3	
	0527	**算法,代码型**	C		an..3	
	0529	**算法代码表标识符**	C		an..3	
	0591	**填充机制,代码型**	C		an..3	
	0601	**填充机制代码表标识符**	C		an..3	
020	S503	**算法参数**	C	9		1
	0531	**算法参数限定符**	M		an..3	
	0554	**算法参数值**	M		an..512	

注: 1 S503 **为一个参数提供了空间。**S503 **的实际最大次数取决于所使用的算法。参数的顺序是任意的,但在每种情况下,它的实际值由一个代码型的算法参数限定符限定。**

USC **证书**

功能:传递公开密钥及其持有者的凭证。

位置	标记	名称	状态	最大次数	表示	注
010	0536	**证书参考**	C	1	an..35	2
020	S500	**安全标识细目**	C	2		3
	0577	**安全参与方限定符**	M		an..3	
	0538	**密钥名称**	C		an..35	
	0511	**安全参与方标识**	C		an..512	
	0513	**安全参与方代码表限定符**	C		an..3	
	0515	**安全参与方代码表负责机构,代码型**	C		an..3	
	0586	**安全参与方名称**	C		an..35	
	0586	**安全参与方名称**	C		an..35	
	0586	**安全参与方名称**	C		an..35	

030	0545	证书语法和版本,代码型	C	1	an..3	2
040	0505	过滤函数,代码型	C	1	an..3	
050	0507	源字符集编码,代码型	C	1	an..3	4
060	0543	证书源字符集字符总表,代码型	C	1	an..3	5
070	0546	用户权限级	C	1	an..35	
080	S505	用于签名的服务字符	C	5		6
	0551	用于签名的服务字符的限定符	M		an..3	
	0548	用于签名的服务字符	M		an..4	
090	S501	安全日期和时间	C	4		7
	0517	日期和时间限定符	M		an..3	
	0338	事件日期	C		n..8	
	0314	事件时间	C		an..15	
	0336	时差	C		n4	
100	0567	安全状况,代码型	C	1	an..3	1
110	0569	取消原因,代码型	C	1	an..3	1

从属性注释:

1 D5(110,100),如果第一项有,则全有。

2 如果不使用整个证书(包括 USR 段),证书中只有数据元 0536 应是唯一的证书参考,它由证书参考(0536)、标识发布者认证机构的 S500 或标识证书持有者的 S500 组成,并包括其公开密钥名称。在非 EDIFACT 的情况下,证书数据元 0545 也应出现。

3 S500/0538 标识了公开密钥,它或者是该证书持有者的公开密钥,或者是与该证书发布者(认证机构或 CA)签发证书所使用的私有密钥相关的公开密钥。

4 0507 是在签署证书时证书的源字符集编码。如果未规定该值,该字符集编码应与字符集字符总表标准所标识的相一致。

5 0543 是在签署证书时证书的源字符集编码。如果未规定该值,则默认值在交换头中定义。

6 当该证书被传送时,S505 将使用 GB/T 14805.1 中定义的默认服务字符或如果使用了服务串通知,则应是该段中定义的服务字符。当证书被签署时,该数据元可规定所使用的服务字符。如果该数据元未被使用,则服务字符为默认的服务字符。

7 S501 表示与认证过程有关的日期和时间。它有可能出现 4 次:一次是证书产生的日期和时间,一次是证书的有效期开始的日期和时间,一次是证书的有效期截止的日期和时间,一次是取消证书的日期和时间。

USH 安全头

功能:规定了应用于 EDIFACT 结构(即报文/包、组、交换)的安全机制。

位置	标记	名称	状态	最大次数	表示	注
010	0501	安全服务,代码型	M	1	an..3	
020	0534	安全参考号	M	1	an..14	
0030	0541	安全应用范围,代码型	C	1	an..3	1
040	0503	应答类型,代码型	C	1	an..3	
050	0505	过滤函数,代码型	C	1	an..3	
060	0507	源字符集编码,代码型	C	1	an..3	2
070	0509	安全提供者的作用,代码型	C	1	an..3	
080	S500	安全标识细目	C	2		3,4
	0577	安全参与方限定符	M		an..3	
	0538	密钥名称	C		an..35	
	0511	安全参与方标识	C		an..17	
	0513	安全参与方代码表限定符	C		an..3	
	0515	安全参与方代码表负责机构,代码型	C		an..3	
	0586	安全参与方名称	C		an..35	
	0586	安全参与方名称	C		an..35	
	0586	安全参与方名称	C		an..35	
090	0520	安全顺序号	C	1	an..35	
100	S501	安全日期和时间	C	1		5
	0517	日期和时间限定符	M		an..3	
	0338	事件日期	C		n..8	
	0314	事件时间	C		an..15	
	0336	时差	C		n4	

注

1 如果数据元 0541 没有出现,则默认的安全应用范围应是当前的安全头段组和报文体或客体。

2 0507 是在对 EDIFACT 结构进行安全处理时该结构的源字符集编码。如果未规定该值,则该字符集编码与 UNB 段中的语法标识符字符总表所标识的编码相一致。

3 S500 可以出现两次:一次用于安全发起方,另一次用于安全接受方。

4 S500/0538 可用于建立发送方和接受方之间的密钥关系。

5 S501 可用作安全时间标记。它是与安全相关的,并且可以不同于任何可能出现在 EDIFACT 结构中其他地方的日期和时间。它可用来提供顺序完整性。

USR 安全结果

功能:包含安全机制的结果。

位置	标记	名称	状态	最大次数	表示	注
010	S508	确认结果	M	2		1
	0563	确认值限定符	M		an..3	
	0560	确认值	C		An..512	

注：1 对于需要用两个参数来表示结果的签名算法，S508 应出现两次。

对于 RSA 签名，S508 只应出现一次。

对于 DSA 签名，S508 应出现两次。

UST 安全尾

功能：在安全头段组和安全尾段组间建立链接。

位置	标记	名称	状态	最大次数	表示	注
010	0534	安全参考号	M	1	an..14	1
020	0588	安全段的数目	M	1	n..10	

注：1 0534 的值应与相应的 USH 段中的 0534 的值相同。

B2 复合数据元目录

B2.1 复合数据元规范说明：

位置：复合数据元中的成分数据元的顺序位置号。

标记：复合数据元目录中的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：成分数据元的英文名称用小写字母表示。

状态：复合数据元中的成分数据元的状态（M 表示必备型，C 表示条件型）。

表示：复合数据元中的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。

说明：复合数据元的描述。

B2.2 从属性注释标识符

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

从属性注释标识符的定义见 GB/T 14805.1—1999 的 11.5。

B2.3 按标记的字母顺序排列的复合数据元索引

标记	名　　称
S500	**安全标识细目**(Security identification details)
S501	**安全日期和时间**(Security date and time)
S502	**安全算法**(Security algorithm)
S503	**算法参数**(Algorithm parameter)
S505	**用于签名的服务字符**(Service character for signature)
S508	**确认结果**(Validation result)

B2.4 按英文名称的字母顺序排列的复合数据元索引

标记	名　　称
S503	**算法参数**(Algorithm parameter)
S502	**安全算法**(Security algorithm)
S501	**安全日期和时间**(Security date and time)
S500	**安全标识细目**(Security identification details)
S505	**用于签名的服务字符**(Service character for signature)
S508	**确认结果**(Validation result)

B2.5 复合数据元规范

S500 **安全标识细目**

说明:在安全过程中涉及的各参与方的标识。

位置	标记	名称	状态	最大次数	表示	注
010	0577	**安全参与方限定符**	M		an..3	
020	0538	**密钥名称**	C		an..35	
030	0511	**安全参与方标识**	C		an..17	1
040	0513	**安全参与方代码表限定符**	C		an..3	1
050	0515	**安全参与方代码表负责机构,代码型**	C		an..3	
060	0586	**安全参与方名称**	C		an..35	
070	0586	**安全参与方名称**	C		an..35	
080	0586	**安全参与方名称**	C		an..35	

从属性注释:

1 D2(030,040,050),**全有或全无**。

S501 **安全日期和时间**

说明:与安全相关的日期和时间。

位置	标记	名称	状态	最大次数	表示	注
010	0517	**日期和时间限定符**	M		an..3	
020	0338	**事件日期**	C		n..8	
030	0314	**事件时间**	C		an..15	
040	0336	**时差**	C		n4	

S502 **安全算法**

说明:安全算法的标识。

位置	标记	名称	状态	最大次数	表示	注
010	0523	算法的使用,代码型	M		an..3	
020	0525	密码操作方式,代码型	C		an..3	1,3
030	0533	操作方式代码表标识符	C		an..3	1,6
040	0527	算法,代码型	C		an..3	2,3,5
050	0529	算法代码表标识符	C		an..3	2
060	0591	填充机制,代码型	C		an..3	4,5
070	0601	填充机制代码表标识符	C		an..3	4

从属性注释:

1 D5(030,020),如果第一项有,则全有。

2 D5(050,040),如果第一项有,则全有。

3 D5(020,040),如果第一项有,则全有。

4 D5(070,060),如果第一项有,则全有。

5 D5(060,040),如果第一项有,则全有。

注:6 操作方式的选择应根据所选定的算法(数据元 0527)进行选择。操作方式与算法的某些组合是不适宜的。

S503 算法参数

说明:安全算法所需的参数。

位置	标记	名称	状态	最大次数	表示	注
010	0531	算法参数限定符	M		an..3	
020	0554	算法参数值	M		an..512	

S505 用于签名的服务字符

说明:计算签名时作为语法服务字符的字符标识。

位置	标记	名称	状态	最大次数	表示	注
010	0551	用于签名的服务字符的限定符	M		an..3	
020	0548	用于签名的服务字符	M		an..4	

S508 确认结果

说明:安全机制的应用结果。

位置	标记	名称	状态	最大次数	表示	注
010	0563	确认值限定符	M		an..3	
020	0560	确认值	C		an..512	

注:1 0560 的长度应由计算确认值的加密算法和应用于结果的过滤函数的特性来决定。

B3 简单数据元目录

B3.1 简单数据元规范说明:

标记: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。

说明: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。

B3.2　按标记排列的简单数据元索引

标记	名　称
0501	**安全服务，代码型**(Security service，coded)
0503	**应答类型，代码型**(Response type，coded)
0505	**过滤函数，代码型**(Filter function，coded)
0507	**源字符集编码，代码型**(Original character set encoding，coded)
0509	**安全提供者的作用，代码型**(Role of security provider，coded)
0511	**安全参与方标识**(Security party identification)
0513	**安全参与方代码表限定符**(Security party code list qualifier)
0515	**安全参与方代码表负责机构，代码型**(Security party code list responsible agency，coded)
0517	**日期和时间限定符**(Date and time qualifier)
0520	**安全顺序号**(Security sequence number)
0523	**算法的使用，代码型**(Use of algorithm，coded)
0525	**密码操作方式，代码型**(Cryptographic mode of operation，coded)
0527	**算法，代码型**(Algorithm，coded)
0529	**算法代码表标识符**(Algorithm code list identifier)
0531	**算法参数限定符**(Algorithm parameter qualifier)
0533	**操作方式代码表标识符**(Mode of operation code list identifier)
0534	**安全参考号**(Security reference number)
0536	**证书参考**(Certificate reference)
0538	**密钥名称**(Key name)
0541	**安全应用范围，代码型**(Scope of security application，coded)
0543	**证书源字符集字符总表，代码型**(Certificate original character set repertoire，coded)
0545	**证书语法和版本，代码型**(Certificate syntax and version，coded)
0546	**用户权限级**(User authorisation level)
0548	**用于签名的服务字符**(Service character for signature)
0551	**用于签名的服务字符限定符**(Service character for signature qualifier)
0554	**算法参数值**(Algorithm parameter value)
0560	**确认值**(Validation value)
0563	**确认值限定符**(Validation value qualifier)
0567	**安全状况，代码型**(Security status，coded)
0569	**取消原因，代码型**(Revocation reason，coded)
0577	**安全参与方限定符**(Security party qualifier)
0586	**安全参与方名称**(Security party name)
0588	**安全段的数目**(Number of security segments)

0591 **填充机制,代码型**(Padding mechanism,coded)

0601 **填充机制代码表限定符**(Padding mechanism code list identifier)

B3.3 按英文名称的字母顺序排列的简单数据元索引

标记	名　称
0529	**算法代码表标识符**(Algorithm code list identifier)
0531	**算法参数限定符**(Algorithm parameter qualifier)
0554	**算法参数值**(Algorithm parameter value)
0527	**算法,代码型**(Algorithm,coded)
0543	**证书源字符集字符总表,代码型**(Certificate original character set repertoire' coded)
0536	**证书参考**(Certificate reference)
0545	**证书语法和版本,代码型**(Certificate syntax and version,coded)
0525	**密码操作方式,代码型**(Cryptographic mode of operation,coded)
0517	**日期和时间限定符**(Date and time qualifier)
0505	**过滤函数,代码型**(Filter function,coded)
0538	**密钥名称**(Key name)
0533	**操作方式代码表标识符**(Mode of operation code list identifier)
0588	**安全段的数目**(Number of security segments)
0507	**源字符集编码,代码型**(Original character set encoding,coded)
0601	**填充机制代码表标识符**(Padding mechanism code list identifier)
0591	**填充机制,代码型**(Padding mechanism,coded)
0503	**应答类型,代码型**(Response type,coded)
0569	**取消原因,代码型**(Revocation reason,coded)
0509	**安全提供者的作用,代码型**(Role of security provider,coded)
0541	**安全应用范围,代码型**(Scope of security application,coded)
0513	**安全参与方代码表限定符**(Security party code list qualifier)
0515	**安全参与方代码表负责机构,代码型**(Security party code list responsible agency,coded)
0511	**安全参与方标识**(Security party identification)
0586	**安全参与方名称**(Security party name)
0577	**安全参与方限定符**(Security party qualifier)
0534	**安全参考号**(Security reference number)
0520	**安全顺序号**(Security sequence number)
0501	**安全服务,代码型**(Security service,coded)
0567	**安全状况,代码型**(Security status,coded)
0548	**用于签名的服务字符**(Service character for signature)
0551	**用于签名的服务字符限定符**(Service character for signature qualifier)
0523	**算法的使用,代码型**(Use of algorithm,coded)
0546	**用户权限级**(User authorisation level)
0560	**确认值**(Validation value)
0563	**确认值限定符**(Validation value qualifier)

B3.4 简单数据元规范

本条只包含在 GB/T 14805 **其他部分中未定义的简单数据元**。

0501 安全服务,代码型

说明:所使用的安全服务的规范。

表示:An..3

0503 应答类型,代码型

说明:预期的、来自接收方的应答类型的规范。

表示:an..3

0505 过滤函数,代码型

说明:用于把任一位模式可逆地映射到一个有限的字符集上的过滤函数的标识。

表示:an..3

0507 源字符集编码,代码型

说明:当应用安全机制时,对经安全处理的 EDIFACT 结构进行编码所使用的字符集的标识。

表示:an..3

0509 安全提供者的作用,代码性

说明:与经安全处理的项相关的安全提供者的作用的标识。

表示:an..512

0511 安全参与方标识

说明:根据定义好的安全参与方记录,安全过程中所涉及的参与方的标识。

表示:an..17

0513 安全参与方代码表限定符

说明:用于注册安全参与方的标识类型的标识。

表示:an..3

0515 安全参与方代码表负责机构,代码型

说明:负责安全参与方注册的机构的标识。

表示:an..3

0517 日期和时间限定符

说明:日期和时间类型的规范。

表示:an..3

0520 安全顺序号

说明:给经安全处理的 EDIFACT 结构所分配的顺序号。

表示:an..35

注:该顺序号是与安全相关,它可以不同于可能出现于 EDIFACT 结构其他地方的 EDIFACT 结构标识。当需要顺序完整性时,可使用它。

0523 算法的使用,代码型

说明:由算法所产生的用法的规范。

表示:an..3

0525 密码操作方式,代码型

说明:用于算法的操作方式的规范。

表示:an..3

0527 算法,代码型

说明:算法的标识。

表示:an..3

0529 算法代码表标识符

说明:用于标识算法的代码表的规范。

表示:an..3

0531 算法参数限定符

说明:参数值类型的规范。

表示:an..3

0533 操作方式代码表标识符

说明:用于标识密码操作方式的代码表的规范。

表示:an..3

0534 安全参考号

说明:由安全发起方给一对安全头和安全尾段组指定的唯一参考号。

表示:an..14

注:该值可以任意指定,但在同一 EDIFACT 结构(如交换、组、报文或包)中不能再重复使用。

0536 证书参考

说明:认证机构用来标识一个证书。

表示:an..35

0538 密钥名称

说明:用于建立参与方之间的密钥关系的名称。

表示:an..35

0541 安全应用范围,代码型

说明:安全头中所定义的安全服务应用范围的规范。

表示:an..3

注:它定义了在相关加密过程中必须考虑的数据。

0543 证书源字符集字符总表,代码型

说明:签署证书时用于创建证书的字符集字符总表的标识。

表示:an..3

0545 证书语法和版本,代码型

说明:用于创建证书的语法和版本的代码型标识。

表示:an..3

0546 用户权限级

说明:与证书持有者相关的权限级的规范。

表示:an..35

0548 用于签名的服务字符

说明:计算签名时使用的服务字符。

表示:an..4

注:为了避免翻译问题,该服务字符用其在源字符集编码数据元(0507)标识的字符集中的值表示。对至少两个字符进行六层过滤。例如,如果使用 GB/T 1988(即 ASCII 编码)8 位编码页,服务字符"/"的编码为"27"(两个字符)。

0551 用于签名的服务字符限定符

说明:计算签名时使用的服务字符类型的标识。

表示:an..3

0554 算法参数值

说明:算法所需的参数的值。

表示:an..512

注:如果需要,该值应由一个适当的过滤函数过滤。注意,密钥名称无须过滤。

0560 **确认值**

说明:与规定的安全功能相对应的安全结果。

表示:an..512

注:如果需要,该值应由一个适当的过滤函数过滤。

0563 **确认值限定符**

说明:确认值类型的标识。

表示:an..3

0567 **安全状况,代码型**

说明:安全元素(如密钥或证书)状况的标识。

表示:an..3

0569 **取消原因,代码型**

说明:取消证书的原因的标识。

表示:an..3

0577 **安全参与方限定符**

说明:安全参与方的作用的标识。

表示:an..3

0586 **安全参与方名称**

说明:安全参与方的名称。

表示:an..35

0588 **安全段的数目**

说明:当一对安全头/尾组被用于加密时,这对安全头/尾组中的安全段的数目,安全段数目应加上 USD 和 USU 段。

表示:n...10

注

1 每对安全头/安全尾组中应包括在这对安全头/安全尾组内的安全段数目的计数。

2 安全段的数目的计数应包括 USR 段。

0591 **填充机制,代码型**

说明:所用的填充机制或填充方案。

表示:an...3

0601 **填充机制代码表标识符**

说明:用来标识填充机制或填充方案的代码表的规范。

表示:an...3

附 录 C
(提示的附录)
EDIFACT 的安全威胁和解决方案

本附录描述了在报文/包的发起方和接受方之间对报文/包传送的一般安全威胁,同时也描述了克服这些威胁的一般方法。在报文/包、组或者交换的任意级上这些威胁和解决方案都是适用的。

C1 安全威胁

通过电子媒体和电子手段存储和传送的 EDIFACT 报文/包会面临一些威胁，主要包括：

——报文/包内容未经授权的泄露；

——虚假报文/包的故意插入；

——报文/包的复制、丢失或重放；

——报文/包内容的篡改；

——报文/包的删除；

——发送方或者接收方对报文/包责任的抵赖。

当未经授权而处理报文/包的内容时，这些威胁可能是有意地造成的；或者当通信错误导致报文/包内容的改变时，这些威胁可能是无意地造成的。

C2 安全解决方案——基本服务和使用原则

为了克服上述威胁，一些安全机制已被标识。这些机制利用一种或多种方法来达到安全目的。

当对报文/包进行安全处理时，重要的是要能够无歧义地标识所涉及到的各参与方——安全发起方（以下简称发送方，在传输之前对报文/包进行安全处理）、安全接受方（以后简称接收方，对接收到的报文/包进行核查）。这些参与方可以在安全段中识别。如果使用非对称算法，则此识别可借助证书（即证书本身或证书参考）来完成。

在开放系统中通常需要认证机构（CA）。它是参与方在有限程度上信任的第三方，负责用公开密钥来标识和注册所有用户。这些识别信息通过证书传递给其他用户，此证书是 CA 对报文签署数字签名，该报文由用户标识信息和用户公开密钥组成。在这种情况下，信任纯粹是功能性的，并不涉及秘密密钥或者私有密钥。

另一方面，如果使用对称算法，有关的参与方的标识应在安全发送方/接收方名称字段中指明。

若干参与方均可对报文/包进行安全处理（如：一个报文/包可以有多个数字签名），因此安全相关信息可被重复，以便允许几个签名方或鉴别方的标识并相应地包括几个数字签名或控制值。

下面给出了对 EDIFACT 报文/包、组或者交换进行安全处理的需求和技术。

C2.1 顺序完整性

顺序完整性防止对 EDIFACT 结构（报文/包、组或者交换）的复制、增加、删除、丢失或者重放。

为了检测到丢失的报文/包、组或者交换

——发送方可以包括一个顺序号（与两个参与方的报文流/包流有关），并由接收方对其进行核查；

——发送方可请求并核查一个确认。

为了检测到增加或者复制的报文/包、组或者交换

——发送方可以包括一个顺序号，并由接收方对其进行核查；

——发送方可以包括一个时间标记，并由接收方对其进行核查。

当使用顺序号时，参与方之间要协商如何管理这些顺序号。

时间标记通常由发送方的系统产生。这意味着，同有纸贸易一样，时间标记的初始精确性只受发送方的控制。

为了给出全面的保护，时间标记或者顺序号的完整性由下述其他功能中的一个来保证。

C2.2 内容完整性

内容完整性防止对数据的篡改。

这种保护可通过发送方加入一个完整性控制值的方法来获得。该值可使用一个适当的加密算法来计算，如一个 MDC（更改检测码）。由于这个控制值本身没有被保护，在控制值上附加一些保护措施是必要的，如：用一个单独途径传递控制值或者计算数字签名，这实际上提供了源抗抵赖性。另一方面，使用

报文鉴别码得到的源鉴别也隐含了内容完整性。接收方使用相应的算法和参数计算接收到的数据的完整性控制值并将结果与实际收到的完整性控制值进行比较。

总之,在 EDI 中内容完整性通常可作为源鉴别或源抗抵赖性的副产品来获得。

C2.3 源鉴别

源鉴别保护接收方以防报文/包、组、或者交换的实际发送方声明是另一(被授权的)参与方。

这种保护可通过加入一个鉴别值(如 MAC:报文鉴别码)来获得。这个值不仅依赖于数据内容,而且依赖于发送方持有的秘密密钥。

本服务包括内容完整性并可作为源抗抵赖性的副产品来获得。

在大多数情况下,应至少采用源鉴别的服务。

C2.4 源抗抵赖性

源抗抵赖性保护报文/包、组或者交换的接收方以防发送方对所发送信息的抵赖。

这种保护可通过加入数字签名(或者使用以防拆硬件或信任第三方的源鉴别的方式描述的函数)来获得。数字签名则可通过利用非对称算法和私有密钥对客体或数据的控制值(如使用散列函数)进行加密而获得。

数字签名可使用公开密钥验证,此公开密钥与创建数字签名的私有密钥相对应。该公开密钥可以包含在参与方签署的交换协定中,也可以包含在认证机构数字签发的证书中。证书可被作为 EDIFACT 结构中的一部分发送。

数字签名不仅提供源抗抵赖性,而且也提供内容完整性和源鉴别。

C2.5 接收的抗抵赖性

接收的抗抵赖性保护报文/包、组或者交换的发送方以防接收方对所接收信息的抵赖。

这种保护可通过接收方发送一个确认来实现。此确认包括一个对原始 EDIFACT 结构中数据的数字签名。该确认采用从接收方到发送方服务报文的形式。

C2.6 内容保密性

内容保密性防止对报文/包、组或者交换内容的非授权的读、拷贝或者泄露。

这种保护可通过加密数据来实现。使用带秘密密钥的对称算法完成加密,发送方和接收方共享此密钥。

而且,该秘密密钥可以通过使用接收方公开密钥的非对称算法进行加密后被传输。

保密性在 GB/T 14805.7 中单独阐述。

C2.7 安全服务间的相互关系

正如已指出的,有些服务在本质上包含其他服务,这样就没有必要额外地包括已隐含获得的服务。例如:源抗抵赖性隐含了内容完整性。

下表总结了这些相互关系:

服务 \ 隐含的服务	内容完整性	源鉴别	源抗抵赖性
内容完整性	是		
源鉴别	是	是	
源抗抵赖性	是	是	是

附 录 D
(提示的附录)
如何保护 EDIFACT 结构

下面是为了实现 EDIFACT 结构如报文/包、组或者交换的安全而采取的一些较为基本的步骤。要

了解进一步的细节和原则性解释，请参考本标准的附录 C、GB/T 9387.2 和 GB/T 16264.8。

第一步（与业务伙伴共同）确定安全服务的要求。下面再次列出 EDIFACT 环境中可利用的安全服务，而且为了防范已标识出的威胁，在业务关系中明确需要哪些服务显得尤为重要。通常，这些需求能够通过审计请求在内部或外部加以定义。发送方可采用的基本安全服务如下：

——内容完整性；

——源鉴别；

——源抗抵赖性。

这些服务不是独立的，因此不必另外包含由其他服务已隐含实现的服务。例如：源抗抵赖性服务隐含了内容完整性。

在附录 C 的 C2.7 中相互关系表中归纳了这些关系。

因此，发送方最多可选择三个服务中的一个。

接收的抗抵赖性是由接收方发起的服务。该服务可由发送方明确请求或者在交换协定中规定。用于传递接收确认的 AUTACK 报文已制定出。

D1 双边协定/第三方

如果要集成安全服务，必须同各业务伙伴制定附加的协定。有许多不同的方法可供使用，这里仅简述两种极端情况下的方法。

最小的需求应是每个参与方就安全服务、算法、代码、密钥管理方法、误操作处理等方面达成双边协定。这样一个协定的草案可从 EC TEDIS 项目中获得。在这种情况下，报文/包本身只需包括很少的安全相关信息。

另一种极端的情况是涉及到作为认证机构的第三方，此认证机构注册所有用户并发布证书来认证用户的公开密钥。在这种情况下，只要同认证机构达成一份协定就足够了。认证机构还应开列黑名单。此时，有必要包括更复杂的安全相关信息。

安全服务已通过一种能提供最大灵活性的方式集成到了 EDIFACT 中，并能满足以上提到的两种极端情况或它们中间的任何情况。

D2 实际方面

当然，为实现这些安全服务需要阐述许多不同方面的内容，例如：密钥生成、对翻译器处理安全段能力的要求、充分利用安全服务的内部过程（如存储收到的带数字签名的报文/包、多个签名的应用等）。

需要强调的是，安全服务的集成是完全透明和独立于所使用的通信协议。如果系统允许传输一个 EDIFACT 报文/包，它也允许传输一个经安全处理的 EDIFACT 报文/包。

D3 构造经安全处理的 EDIFACT 结构的过程

首先，创建一个 EDIFACT 结构的报文/包、组或交换，第二步是确定和应用适当的安全服务。如果这些服务是基于数字签名的，就将直接或者间接地涉及到私有密钥持有者。在 EDIFACT 结构生成后，第二步不必立即进行。

类似地，在处理收到的 EDIFACT 结构时，第一步要验证安全服务，就像有纸贸易一样尽可能存储经安全处理的 EDIFACT 结构以供今后审计和归档。

D4 安全服务的应用顺序

安全服务执行的顺序完全由用户决定，因为所有的服务彼此间是完全独立的。特别是，如果使用多个签名且没有嵌入安全头段组和安全尾段组，这些签名的计算和验证顺序是无关紧要的。

D5 报文/包级上分离报文的安全

该特性有两个业务需求：

a) 以来自发送方单个分离报文的方式为一个或多个报文/包提供安全服务；

b) 为发送方提供经安全处理的确认(收到原始报文/包而不作返回)。

安全鉴别和确认报文 AUTACK(GB/T 14805.6)可满足这些需求。

D5.1 发送方使用的分离报文的安全

AUTACK 的这种使用允许发送方提供任何安全服务，但以一个分离报文的形式发送。这样安全服务可在以后或者更合适阶段传输。此外，同样在报文/包级上，相对于直接集成一次仅能对一个报文/包进行安全处理而言，他们可以对若干原始报文/包进行安全处理。

对集成的和分离的方法而言其原则是等同的，但是分离方法需要给予安全处理的原始报文/包一个唯一参考。

D5.2 接收方使用的分离报文的安全

AUTACK 的这种使用描述了提供接收的抗抵赖性的需求。AUTACK 的详尽描述，参见 GB/T 14805.6。

AUTACK 可作为经安全处理的确认来使用。该确认由一个或多个交换、或者一个或多个交换中的一个或多个报文/包的接收方发送给发送方。生成 AUTACK 的准则和方法向原始报文/包或者交换的发送方提供经安全处理的确认，即原始报文/包或交换已经被预定方收到。

D6 组或交换级上分离报文的安全性

D5 部分中描述的分离的报文/包安全性可用于保证整个组或整个交换。

本特性的两种业务需求是：

a) 以来自发送方单个分离报文的方式为一个或多个组/交换提供安全服务；

b) 为发送方提供经安全处理的确认(收到原始报文/包而不作返回)。

GB/T 14805.6 描述的安全鉴别和确认报文 AUTACK，可满足这些需求。

附 录 E
(提示的附录)
报文保护示例

本附录提供三个示例以说明安全服务段的不同应用。

这些报文安全的示例基于 SWIFT 发布的金融报文的报文实施指南中描述的 EDIFACT 付款通知。然而这里描述的安全机制与报文类型无关，并且可适用于任何 EDIFACT 报文。

“示例 1：报文源鉴别”说明了当应用一个基于对称算法的方法时，如何使用安全服务段来提供报文源鉴别。伙伴间事前已交换对称密钥，并且安全头段组只包含两个相当简单的段。

“示例 2：源抗抵赖性，方法一”说明了当应用一个基于非对称算法的方法时，如何使用安全服务段来提供源抗抵赖性。直接用于报文的算法是一个散列函数，此散列函数不需要在伙伴之间交换任何密钥。散列值由一个非对称算法来签发。验证报文签名的接收方所需的公开密钥包含在一个证书段中，并在报文的安全头段组中传递此证书段。为了使任何伙伴都能验证证书的完整性和真实性，这个证书由它的发布者(“AUTHORITY”)签发并包括授权的公开密钥。

“示例 3：源抗抵赖性，方法二”说明了当应用一个基于非对称算法的方法时，如何使用安全服务段来提供源抗抵赖性。直接用于报文的算法是一个对称算法，这需要在伙伴间交换对称密钥，该算法并提供一个“完整性值”。该对称密钥通过报文的安全头段组进行交换，并且通过非对称算法用预定接收方的

公开密钥加密。

完整性值用非对称算法签发。验证报文签名的接收方所需的公开密钥包含在第一个证书段中，并在报文的安全头段组中传递此证书段。为了使任何伙伴都能验证证书的完整性和真实性，这个证书由它的发布者("AUTHORITY")签发并包括该机构的公开密钥。

第二个证书段包含对预定接收方公开密钥的参考，并由报文发送方用来保护对称密钥。本技术目前在法国银行的 ETEBAC5(银行和客户间经安全处理的文件的传送)系统中使用。

在后两个例子中，信任机构的任何伙伴都可以只使用报文中包含的数据来验证所收到报文的签名。

E1 示例 1：报文源鉴别

E1.1 概述

1996 年 4 月 9 日，A 公司委托 A 银行(分类代码为 603000)，记入它的借方帐号 00387806 款值 54345.10 英镑。此款项要付给 B 银行(分类代码是 201827)中，West Dock，Milford Haven 的 B 公司的帐号 00663151。付款以发票 62345 结算，收款人是销售部的 Jones 先生。

A 银行要求用"报文源鉴别"的安全功能来对该付款通知进行安全处理。

这种要求是通过报文发送方根据 ISO 8731-1 使用"数据加密标准"(DES)生成的"报文鉴别码"(MAC)来实现的，并且该代码要由 A 银行进行验证。假定在 A 公司和 A 银行间秘密 DES 密钥已被事先交换。

注：下面只提及报文中与安全相关的部分。

E1.2 安全细目

安全头	
安全服务	报文源鉴别
安全参考号	本安全头的参考号是 1
过滤函数	所有的二进制值(MAC)用十六进制过滤器过滤
源字符集编码	当生成 MAC 时，报文用 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(生成报文鉴别码的参与方)	A 公司的 Smith 先生
安全标识细目 报文接收方(验证报文鉴别的参与方)	A 银行
安全顺序号	本报文的安全顺序号是 001
安全日期和时间	安全时间标记是：日期：1996 年 4 月 9 日　时间：13：59：50
安全算法	
安全算法 算法的使用 密码的操作方式 算法	 使用对称算法得到报文源鉴别 根据 ISO 8731-1 计算 MAC 使用 DES 算法
算法参数 算法参数限定符 算法参数值	 标识下列算法参数值为预先交换的秘密密钥的名称 使用称为 MAC-KEY1 的密钥
安全尾	
安全参考号	本安全尾的参考号是 1
安全段的数目	4
安全结果	
确认结果 确认值限定符 确认值	 MAC 4 字节确认结果(报文鉴别码)

E2 示例 2:源抗抵赖性,方法一

E2.1 概述

A 银行要求由 A 公司的 Smith 先生对付款通知实施源抗抵赖性的安全服务。

参与方之间的交换协定规定:A 银行所要求的源抗抵赖性安全服务应由 A 公司的 Smith 先生使用带有数字签名的付款通知来实现。

标识 Smith 先生公开密钥的证书由一个双方都信任的认证机构(即证书发布者)签发。

E2.2 安全细目

安全头	
安全服务	源抗抵赖性
安全参考号	本安全头的参考号是 1
应答类型	不需要确认
过滤函数	用十六进制过滤器过滤所有的二进制值(签名)
源字符集编码	当生成签名时,报文用 GB/T 1988(即 ASCII 码)8 位进行编码
安全顺序号	本报文的安全顺序号是 202
安全日期和时间	安全时间标记是:日期:1996 年 1 月 15 日 时间:10 : 05 : 30
安全算法	Smith 先生签名用的散列函数
安全算法 算法的使用 密码的操作方式 算法	 使用持有者的散列算法 使用适宜的散列函数(ISO/IEC 10118-2《使用 n 位块密码算法的散列函数》)来提供双倍长度的散列代码(128 位);初始化值: V=0F 0F 0F 0F 0F 0F 0F 0F IV′=F0 F0 F0 F0 F0 F0 F0 F0; 使用 DES 块密码算法
证书	Smith 先生的证书
证书参考	本证书由 AUTHORITY 参考:00000001
安全标识细目 证书持有者	 A 公司的 Smith 先生
安全标识细目 证书发布者 密钥名称	 Smith 先生的证书由称为“AUTHORITY”的认证机构生成 AUTHORITY 用于生成 Smith 先生证书的公开密钥是 PK1
证书语法和版本	UN/EDIFACT 服务段目录的证书版本
过滤函数	所有的二进制值(密钥和数字签名)用十六进制过滤器来过滤
源字符集编码	当生成证书时,证书以 GB/T 1988(即 ASCII 码)8 位进行编码
用于签名的服务字符 用于签名的服务字符限定符 用于签名的服务字符	计算签名时使用的服务字符 服务字符是段终止符 值“'”(撇号)
用于签名的服务字符 用于签名的服务字符限定符 用于签名的服务字符	计算签名时使用的服务字符 服务字符是数据段分隔符 值“+”(加号)

用于签名的服务字符 用于签名的服务字符限定符 用于签名的服务字符	计算签名时使用的服务字符 服务字符是成分数据元分隔符 值“:”(冒号)
用于签名的服务字符 用于签名的服务字符限定符 用于签名的服务字符	计算签名时使用的服务字符 服务字符是重复分隔符 值“*”(星号)
用于签名的服务字符 用于签名的服务字符限定符 用于签名的服务字符	签名被计算时使用的服务字符 服务字符是释放字符 值“?”(问号)
安全日期和时间 日期和时间	证书产生时间 Smith 先生的证书在 93 年 12 月 15 日 14：12：00 生成
安全日期和时间 日期和时间	证书有效期的生效时间 Smith 先生证书有效期的生效时间是:1996 01 01 00：00：00
安全日期和时间 日期和时间	证书有效期的截止时间 Smith 先生证书有效期的截止时间是:1996 12 31 23：59：59
安全算法	Smith 先生签名用的非对称算法
安全算法 算法的使用 密码的操作方式 算法	 使用持有者签名算法 这里没有相关的操作方式 RSA 是非对称算法
算法参数 算法参数限定符 算法参数值	 标识这个算法参数为一个签名验证的公共指数 Smith 先生的公开密钥
算法参数 算法参数限定符 算法参数值	 标识这个算法参数为一个签名验证的模数 Smith 先生的模数
算法参数 算法参数限定符 算法参数值	 标识这个算法参数为 Smith 先生模数(用位表示)的长度 Smith 先生模数的长度是 512 位
安全算法	AUTHORITY 用来生成 Smith 先生证书的散列函数
安全算法 算法的使用 密码的操作方式 算法	 使用发布者的散列算法 使用适宜的散列函数(ISO/IEC 10118-2《使用 n-位块密码算法的散列函数》)来提供双倍长度的散列代码(128 位);初始化值: IV＝0F 0F 0F 0F 0F 0F 0F 0F IV′＝F0 F0 F0 F0 F0 F0 F0 F0;按 ISO/IEC 10118-2 的 B3.1 段的规定作为填充规则,按 ISO/IEC 10118-2 的附录 A 中的规定转换 u 和 u′。 使用 DES 块密码算法
安全算法	AUTHORITY 签名用的非对称算法
安全算法 算法的使用 密码的操作方式 算法	 使用发布者签名算法 这里没有相关的操作方式 RSA 是非对称算法

算法参数 算法参数限定符 算法参数值	 标识这个算法参数为一个签名验证的公共指数 AUTHORITY 的公开密钥
算法参数 算法参数限定符 算法参数值	 标识这个算法参数为一个签名验证的模数 AUTHORITY 的模数
算法参数 算法参数限定符 算法参数值	 标识这个算法参数为一个认证机构的模数 AUTHORITY 的模数长为 512 位
安全结果	证书的数字签名
确认结果 确认值限定符 确认值	 数字签名 512 位的数字签名
安全尾	
安全参考号	本安全尾参考号是 1
安全段的数目	9
安全结果	报文的数字签名
确认结果 确认值限定符 确认值	 数字签名 512 位的数字签名

E3 示例 3:源抗抵赖性,方法二

E3.1 概述

A 银行要求 A 公司的 Smith 先生对付款通知实施源抗抵赖性的安全服务。

A 公司要求 A 银行的一个安全确认(接收的抗抵赖性),这将在 AUTACK 报文中传递。

参与方之间的交换协定规定:源抗抵赖性安全服务可通过带有数字签名的付款通知来实现。

双方都同意在 CBC 操作方式的 DES 计算出的 64 位整数值上用 512 位 RSA(非对称算法)计算这个签名。标识 Smith 先生公开密钥的证书被一个双方都信任的认证机构签发。

E3.2 安全细目

安全头	
安全服务	源抗抵赖性
安全参考号	本安全头的参考号是 1
应答类型	要求确认
过滤函数	用十六进制过滤器过滤所有的二进制值(签名)
源字符集编码	当生成报文签名时,报文用 GB/T 1988(即 ASCII 码)8 位进行编码
安全标识细目 报文发送方(保护报文的一方)	 A 公司的 Smith 先生
安全标识细目 报文接收方(验证报文安全的一方)	 A 银行
安全顺序号	本报文的安全顺序号是 001
安全日期和时间	安全时间标记是:日期:1996 01 15　时间:10:05:30

安全算法	用于计算一个完整值的对称算法
安全算法 算法的使用 密码的操作方式 算法	 使用持有者的散列算法 密码块链接;即 ISO 10116(n 位)。计算 64 位完整值;初始化值是二进制 0;使用 DES 秘密密钥。在 A 银行公开密钥下加密传输。 使用 DES 块密码算法
算法参数 算法参数限定符 算法参数值	 标识下列算法参数值为由公开密钥加密的对称密钥 由 A 银行公开密钥加密的对称密钥
算法参数 算法参数限定符 算法参数值	 标识下列算法参数值为清除文本初始化值 清除文本初始化值(所有二进制 0 的)
证书	Smith 先生的证书(报文发送方)
证书参考	本证书由 AUTHORITY 参考:00000001
安全标识细目 证书持有者	 A 公司的 Smith 先生
安全标识细目 证书发布者 密钥名称	 Smith 先生的证书由认证机构 AUTHORITY 生成 用于生成 Smith 先生证书的 AUTHORITY 公开密钥是 PK1
证书的语法和版本	UN/EDIFACT 服务段目录的证书版本
过滤器功能	所有的二进制值(密钥和数字签名)用十六进制过滤器过滤
源字符集编码	当生成证书时,证书使用 GB/T 1988(即 ASCII 码)8 位进行编码
用于签名的服务字符 用于签名的服务字符限定符 用于签名的服务字符	计算签名时使用的服务字符 服务字符是段终止符 值“'”(撇号)
用于签名的服务字符 用于签名的服务字符限定符 用于签名的服务字符	计算签名时使用的服务字符 服务字符是数据段分隔符 值“+”(加号)
用于签名的服务字符 用于签名的服务字符限定符 用于签名的服务字符	计算签名时使用的服务字符 服务字符是成分数据元分隔符 值“:”(冒号)
用于签名的服务字符 用于签名的服务字符限定符 用于签名的服务字符	计算签名时使用的服务字符 服务字符是重复分隔符 值“*”(星号)
用于签名的服务字符 用于签名的服务字符限定符 用于签名的服务字符	计算签名时使用的服务字符 服务字符是发布字符 值“?”(问号)
安全日期和时间 日期和时间	证书生成时间 Smith 先生的证书在 1993 12 15　14:12:00 产生
安全日期和时间 日期和时间	证书有效期的生效 Smith 先生有效期的生效时间是:1996 01 01　00:00:00
安全日期和时间 日期和时间	证书有效期的截止时间 Smith 先生有效期的截止时间是:1996 12 31　23:59:59
安全算法	Smith 先生签名用的非对称算法

安全算法 算法的使用 密码的操作方式 算法	 使用持有者签名算法 这里没有相关的操作方式 RSA 是非对称算法
算法参数 算法参数限定符 算法参数值	 标识本算法参数为签名验证的公共指数 Smith 先生的公开密钥
算法参数 算法参数限定符 算法参数值	 标识本算法参数为签名验证的模数 Smith 先生的模数
算法参数 算法参数限定符 算法参数值	 标识本算法参数为 Smith 先生模数(用位表示)的长度 Smith 先生模数的长度为 512 位
安全算法	AUTHORITY 生成 Smith 先生证书所使用的散列函数
安全算法 算法的使用 密码的操作方式 算法	 使用发布者的散列算法 RSA n 位平方模　GB/T 16264.8 附录 D。 RSA 非对称算法
安全算法	AUTHORITY 签名所用的对称算法
安全算法 算法的使用 密码的操作方式 算法	 使用发布者签名算法 这里没有相关的操作方式 RSA 是非对称算法
算法参数 算法参数限定符 算法参数值	 标识本算法参数为签名验证的公共指数 AUTHORITY 的公开密钥
算法参数 算法参数限定符 算法参数值	 标识本算法参数为签名验证的模数 AUTHORITY 的模数
算法参数 算法参数限定符 算法参数值	 标识本算法参数为 AUTHORITY 模数(用位表示)的长度 AUTHORITY 模数的长度为 512 位
安全结果	证书的数字签名
确认结果 确认值限定符 确认值	 数字签名 512 位数字签名
证书	A 银行(报文接收方)的证书
证书参考	使用与证书参考 00001001 有关的 A 银行的公开密钥
安全尾	
安全参考号	本安全尾的参考是 1
安全段的数目	10
安全结果	报文的数字签名
确认结果 确认值限定符 确认值	 数字签名 512 位数字签名

附 录 F
（提示的附录）
用于 UN/EDIFACT 字符集字符总表 A 和 C 的过滤函数

F1 EDA 过滤器

F1.1 基本原理

十六进制过滤函数将表示二进制数据所需的字符数增加了一倍，这浪费了空间。其他现有的标准化的过滤函数或是因为这些函数将 UN/EDIFACT 字符集 A 和 B 映射为几乎全部可打印的 ISO 字符集（即 96 个可打印字符集中的 94 个），或是因为他们没有比十六进制过滤（博多过滤器）更多的有效空间而不适用于 UN/EDIFACT 字符集 A 和 B。因此建议定义一个简单的过滤函数，该函数能映射到 UN/EDIFACT A 级字符集字符总表（或子集）并且比十六进制过滤器更有效。

F1.2 UN/EDIFACT 字符集字符总表

字符集字符总表 A 拥有 44 个不受使用限制的字符。除 44 个字符外，4 个服务字符和 8 个电传传输所不允许的字符也是该字符集的一部分。

所有这些字符也是 UN/EDIFACT 字符集字符总表 B 的一部分，该字符集不是用于电传传输的，它拥有 82 个常规字符和 3 个不可打印的服务字符。

F1.3 2 被 3 过滤

用 3 个过滤字符表示 2 个二进制字符；在字符集中至少需要 41 个字符：

$41^3 = 68\ 921 > 65\ 536 > 64\ 000 = 40^3$

F1.4 EDA 过滤器规范

假设允许使用 44 个字符，通过以下的方法能使我们避免使用这 44 个字符的字符位置并且过滤每对输入的字符（如果输入数据为奇数，则仅过滤在 2 个结果字符中的最后一个字符）：

——考虑由字符对所组成的无符号整数的二进制值（该值通常取决于应用中计算机的 LITTLE-ENDIAN/BIG-ENDIAN（即最低位或者最高位）特性，BIG-ENDIAN 的标准：第一字节有效）。

——在 0～42 之间，用连续 3 个数（2 个表示最后的奇数字节）表示数值。这三个数是：

1）数值被 1849（即 43 的平方）除的模数（最后的奇数字节可省略）。

2）数值对 1849 整除的余数取 43 的模数。

3）数值对 43 的模数。

——将每个数值按相应的对照表映射到 UN/EDIFACT A 级字符集中：

0～9	由 0～9 表示；
A—Z	由 10～35 表示；
( ),—. /=	由 36～42 按给定的顺序表示。

F1.5 消过滤

消过滤：把 43 字符的每个映射回它的值 0～42。

如果至少保留 3 位过滤字符，计算：$c1 * 1849 + c2 * 43 + c3$ = 短整数

否则至少保留 2 位，计算：$c1 * 43 + c2$ = 字符值

注

1 短整数结果应小于 65536。

2 字符结果应小于 256。

3 在 LITTLE _ ENDIAN 计算机中，转换短整数结果的 2 位字符。

F2 EDC 过滤器

F2.1 基本原理

EDA 过滤器的开发是为了允许过滤 EDIFACT A 或 B 级字符总表。当然，由于该字符总表在字符中有限，3/2 扩充率是相当不理想的，尽管这比 2/1 的十六进制过滤器已经好多了。

在 C、D、E 和 F 字符总表，很容易完成一个更好的扩充率。

实际上，在这些字符总表，不允许的组合仅包括二进制值 0/0～1/15 和值 8/0～9/15。

在 256 个可能的二进制值中 192 个是允许的。

一个 C 级过滤器，低扩充率是理想的，但是需要冗长的计算，将允许把 18 个二进制字节表示成 19 个过滤字节，但不是 19 个字节变成 20 个过滤字节，因为：

$192^{19} > 256^{18}$ 及，

$192^{20} > 256^{19}$

把传输限制到位操作，8/7 的扩充率是可行的。

F2.2 过滤变换

把一个二进制串字节的字符变换成 C 级字符总表：

——细分 7 字节的子字符串（最后的子字符串最多有 7 个字节）；

——在每个子字符串前添加一个开始值 64（位 1=1）的控制字节；

——在控制字节的每位加 1，0 位或者 2 位或 7 位，根据过滤变换是不是用于相应的子字符串的数据字节；

——对子字符集串中的每个数据字节验证是否采用了过滤变换（data byte .and. 64==0）；

——如果采用了过滤变换，则在数据字节中和控制字节位置中置 1 位为 1；

——否则保持数据字节和控制字节不变。

注

1 全部过滤值限于每个字节的 1 位置 1。

2 缺省的服务字符不包括在过滤目标字符总表。

F2.3 逆过滤变换

过滤的字符变换回二进制字符串：

——细分 8 字节子字符串的字符串（最后的子字符串最多有 8 个字节）；

——把每个子字符串的起始字节作为控制字节，其余的字节是数据字节；

——验证控制字节的位置 0 和 2～7；

——相应的字节位置分别是子字符串的 1～7；

——如果位=0，保持相应位置的数据字节不变；

——如果位=1，把相应数据字节的位 1 置为 0。

附 录 G
（提示的附录）
服务代码目录*

服务代码目录由 UN/ECE 维护并且是（UNTDID）联合国贸易数据交换目录的一部分。因此在本标准中不重新制定。服务代码目录的新版本应使用简单数据元目录中有代码数据元的参考代码值（见附录 C）。UNTDID 按正常周期推出和公布。

* 修订稿——批准后增加到 GB/T 14805.1 的附录 D 中。

附 录 H
（提示的附录）
安全服务和算法

H1 目的和范围

附录 H 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更广泛使用的安全技术。

本附录不包括可能组合的全集。这里的举例不表示支持某种算法或操作方法。使用者应选择他想保护的安全威胁的技术。

本附录的目的是给选择安全技术的使用者提供制定适合其实际应用的方案。

为便于阅读和理解，本主题被分为两个段落。每个段落集中了应用安全的不同原理。

这两个段落是：

a）采用对称算法和完整性安全段的组合；

b）采用非对称算法和完整性安全段的组合。

0501 安全服务，代码型
1 源抗抵赖性
2 报文源鉴别
3 完整性

0505 过滤函数，代码型
6 UN/EDIFACT EDC 过滤器

0523 算法的使用，代码型
1 持有者散列算法
2 持有者对称算法
3 发布者签名算法(CA)
4 发布者散列算法(CA)
6 持有者签名算法

0525 操作的加密方法，代码型
6 MAC(报文鉴别码)
7 DIM1(数据元完整性机制)
9 MDC2(修改检测代码)
11 HDS2
16 DSMR(报文恢复的数字签名)

0527 算法，代码型
1 DES(数据加密标准)
10 RSA(Rivest，shamir，adleman)
11 DSA(数字签名算法)
16 SHA-1(安全散列算法)

0531 算法参数限定符
5 对称密钥加密
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
25 DSA 参数 P
26 DSA 参数 Q
27 DSA 参数 G
28 DSA 参数 Y

0563 确认值限定符
1 唯一确认值
2 DSA 算法 r 参数
3 DSA 算法 s 参数

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 鉴别参与方

使用的缩写：

a,b,c,d,e	=	表示安全参考号
CA	=	证书认证机构
Enc-Key	=	加密密钥
G	=	G 公开密钥 DSA 参数
Hash	=	散列值
KEK-N	=	加密密钥名称的密钥
Key-N	=	密钥名称
KN	=	密钥名称
MAC	=	报文鉴别码
Mod	=	模数
Mod-L	=	模数长度
P	=	P 公开密钥 DSA 参数
PK/CA	=	认证机构公开密钥
Pub-K	=	公开密钥
Q	=	Q 公开密钥 DSA 参数
R	=	DSA 签名的 r 参数结果
S	=	DSA 签名的 s 参数结果
Sig	=	签名
Y	=	Y 公开密钥 DSA 参数

H2 使用对称算法和完整性安全段的组合

表 H1 为下列特殊情况建立了关系：

——完整性报文/包/组/交换级安全(见 GB/T 14805.5)；

——仅使用对称算法；

——所提供的安全服务是报文源鉴别和内容完整性；

——通过给报文增加一个 MAC(报文鉴别码)来提供报文源鉴别。举两个例子，第一个例子是 DES 的 CBC 方式带有一个只有报文接收方知道的秘密密钥，这个秘密密钥只由密钥名称来引用。第一个例子符合 ISO 8731-1。第二个例子是根据 ISO 9797 所描述的工作方式的 DES 算法的用法。所需的秘密密钥，是通过 DES 用发送方和接收方共用的“密钥加密密钥”加密后来传送的。这个“密钥加密密钥”是通过该密钥名称来引用的；

——内容完整性是通过 DES 算法的散列函数来提供的，该算法使用 ISO 10118-2 的 MDC 方式。在发送方和接收方之间，没有共享安全密钥。散列值传送不受保护，因此，该安全服务可能不能充分地保护报文；

——尽管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命名；

——这里只给出与实际应用的安全技术、算法和操作方式相关的安全字段。

表 H1　仅使用对称算法时的关系矩阵

标记	名　　称	状态	最大次数	报文源鉴别 ISO 8731-1	报文源鉴别 GB 15852	内容完整性 ISO 10118-2	注
SG1		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		2	2	3	
0534	安全参考号	M		a	B	C	
0505	过滤含数,代码型	C		6	6	6	
S500	安全标识细目	C	2				
0577	安全参与方限定符	M		1	1	1	2
0538	密钥名称	C		Key-N	—	—	3
S500	安全标识细目	C	2				
0577	安全参与方限定符	M		2	2	2	4
USA	安全算法	C	3				
S502	安全算法	M	1				
0523	算法使用,代码型	M		2	2	2	
0525	加密方的操作方式,代码型	C		6/*	7/*	9/*	
0527	算法,代码型	C		1/*	1/*	1/*	
S503	算法参数	C	9		1 个用于密钥加密密钥名称		
0531	算法参数限定符	M		—	10	—	5
0554	算法参数值	M		—	KEK-N	—	
S503	算法参数	C	9		1 个用于加密密钥		
0531	算法参数限定符	M		—	5	—	6
0554	算法参数值	M		—	Enc-Key	—	
将安全化的数据结构(用户段/客体/报文/包/组)							
SGn		C	99	每个安全服务 1 个			1
UST	安全尾	M	1				
0534	安全参考数	M		a	B	C	
0588	安全段的数	M					
USR	安全结果	C	1				
S508	确认结果	M	2				7
0563	确认值限定符	M		1	1	1	
0560	确认值	C		MAC	MAC	Hash	8

表 H1(完)

标记	名　　称	状态	最大次数	报文源鉴别 ISO 8731-1	报文源鉴别 GB 15852	内容完整性 ISO 10118-2	注

注

1　这两个结构必须有相同出现次数。

2　报文发送方。

3　发送方和接收方共享的安全密钥名称。

4　报文接收方。

5　由发送方和接收方共享的密钥加密密钥,在此由其名称指出。

6　安全密钥传送具有密钥加密密钥的加密 DES。

7　一些签名算法(像 DSA)需要两个结果参数。

8　完整性的结果值不被保护并且可分开提出。

*　进一步的代码组合是可能的和需要的。

H3　使用非对称密钥和完整性安全段的组合

表 H2 为下列特殊情况建立了关系:

——完整性报文/包/组/交换级安全。

——提供的安全服务是源抗抵赖性,这里列出了两种不同的签名计算方法。

——两种非对称算法:RSA 和 DSA。

——两种散列函数:MDC 方式的 DES 和 RSA 以及 SHA—1 和 DSA。

——假设证书事先未被交换。

——USC 段包含明确的散列函数和认证机构用来签署证书的签名函数的标识。检查证书签名所需的认证机构的公开密钥接收方已经知道。它由 USC 段中的名称指出。

——只包括一个证书,仅当使用接收方的公开密钥时,第二个证书才是必要的。

表 H2　使用非对称算法时的关系矩阵

标记	名　　称	状态	最大次数	源抗抵赖性性(RSA)	源抗抵赖性性(DSA)	注
SG1		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		1	1	2
0534	安全参考号	M		d	e	
0505	过滤函数,代码型	C		6	6	
S500	安全标识细目	C	2			
0577	安全参与方限定符	M		1	1	3
S500	安全标识细目	C	2			
0577	安全参与方限定符	M		2	2	4
USA	安全算法	C	3			
S502	安全算法	M	1			
0523	算法的使用,代码型	M		1	1	5

表 H2(续)

标记	名　　称	状态	最大次数	源抗抵赖性性(RSA)	源抗抵赖性性(DSA)	注
0525	加密操作方式,代码型	C		11/*	—	
0527	算法,代码型	C		1/*	16	
SG2		C	2	仅1个:发送方证书		
USC		M	1			
0536	证书参考	C	1	该证书的参考		
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	3	6
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	4	7
0538	密钥名称	C		(PK/CA name)	(PK/CA name)	
USA	安全算法	C	3	(sender's signature function)		
S502	安全算法	M	1			
0523	算法的使用,代码型	M		6	6	8
0525	密码操作方式,代码型	C		16	—	
0527	算法,代码型	C		10	11	
S503	算法参数,算法参数限定符	C	9	(模数的长度)	DSA 参数 P	
0531	算法参数限定符	M		14	25	
0554	算法参数值	M		Mod-L	P	
S503	算法参数	C	9	(模数)	DSA 参数 Q	
0531	算法参数限定符	M		12	26	
0554	算法参数值	M		Mod	Q	
S503	算法参数	C	9	(公开指数)	参数 G	
0531	算法参数限定符	M		13	27	
0554	算法参数值	M		Pub-K	G	
S503	算法参数	C	9	—	参数 Y	
0531	算法参数限定符	M		—	28	
0554	算法参数值	M		—	Y	
USA	安全算法	C	3	(用于证书签名的 CA 散列函数)		
S502	安全算法	M	1			
0523	算法的使用,代码型	M		4	4	9
0525	密码操作方式,代码型	C		11	—	
0527	算法,代码型	C		1	8	
USA	安全算法	C	3	(用于证书签名的 CA 签名函数)		

表 H2(完)

标记	名　　称	状态	最大次数	源抗抵赖性性(RSA)	源抗抵赖性性(DSA)	注
S502	安全算法	M	1			
0523	算法的使用,代码型	M		3	3	10
0525	密码操作方式,代码型	C		16	—	
0527	算法,代码型	C		10	11	
USR	安全结果	C	1			
S508	确认结果	M	2			11
0563	确认值限定符	M		1	2	
0560	确认值	C		Sig	R	
S508	确认结果	M	2			11
0563	确认值限定符	M		—	3	
0560	确认值	C		—	S	
将经安全处理的数据结果(用户段/客体/报文/包/组)						
SGn		C	99	每个安全服务 1 个		1
UST	安全尾	M	1			
0534	安全参考号	M		d	e	
0588	安全段的号	M				
USR	安全结果	C	1			
S508	确认结果	M	2			11
0563	确认值限定符	M		1	2	
0560	确认值	C		Sig	R	
S508	确认结果	M	2			11
0563	确认值限定符	M		—	3	
0560	确认值	C		—	S	

注

1　这两个结构必须有相同的出现次数。
2　假设报文源鉴别和完整性包括在源抗抵赖性中。
3　报文发送方。
4　报文接收方。
5　经安全处理的结构上由发送方使用的散列函数。
6　证书持有者:标识的细目应与报文发送方 USH S500 中相同。
7　鉴别参与方:认证机构(CA)。
8　发送方签名函数。
9　CA 的散列函数。
10　CA 的签名函数。
11　一些签名算法(例 DSA)需要两个结果参数。
*　进一步代码组合是可能和需要的。

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 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）
GB/T 14805.5—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 3　字数 82 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：155066·1-16675　定价 21.00 元
*
标 目 408—22

GB/T 14805.5-1999