ICS 35.240.60
L 70

中华人民共和国国家标准

GB/T 14805.6—1999
idt ISO 9735-6:1998

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6部分:安全鉴别和确认报文（报文类型为AUTACK）

Electronic data interchange for administration, commerce and transport (EDIFACT)—Application level syntax rules(Syntax version number:4)—Part 6:Secure authentication and acknowledgement message(message type -AUTACK)

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 9735-6:1998《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 6 部分:安全鉴别和确认报文(报文类型为 AUTACK)》。

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 ××××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 是标准的附录,附录 B、附录 C、附录 D 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: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:王颜尊、吴志刚、李颖、张荣静、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 理事会接收为国际标准之前,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。它通过一个安全鉴别和确认报文的方法来提供保护一个 EDIFACT 结构(即报文、包、组或交换)的可选功能。

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6部分：安全鉴别和确认报文（报文类型为AUTACK）

GB/T 14805.6—1999
idt ISO 9735-6:1998

Electronic data interchange for administration, commerce and transport (EDIFACT)—Application level syntax rules(Syntax version number:4)—Part 6:Secure authentication and acknowledgement message(message type-AUTACK)

1 范围

本标准定义了安全鉴别和确认报文（报文类型为AUTACK）。

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 定义

本标准所使用的定义见GB/T 14805.1—1999的附录A和GB/T 14805.5—1999的附录A。

4 安全鉴别和确认报文的使用规则

4.1 功能定义

AUTACK是鉴别发送的交换、组、报文或包的报文，或对所接收到的交换、组、报文或包提供安全确认的报文。

安全鉴别和确认报文能用于：

a）对于报文、包、组或交换提供安全鉴别、完整性或源抗抵赖性。

b）对于经安全处理的报文、包、组或交换提供接收的安全确认或接收的抗抵赖性。

国家质量技术监督局1999-11-11批准　　2000-05-01实施

4.2 应用领域

安全鉴别和确认报文适用于国内贸易和国际贸易。它是基于行政、商业和运输业相关领域内的广泛实践，而不受业务或行业类型的限制。

4.3 原则

所应用的安全规程应由贸易参与方协商通过并应在交换协定中进行规定。

安全鉴别和确认报文(AUTACK)向其他 EDIFACT 结构(包括报文、包、组或交换)实施安全服务，并且对经安全处理的 EDIFACT 结构提供安全确认。它也能应用于贸易双方间需要安全处理的 EDIFACT 结构组合。

安全服务是通过应用于原始 EDIFACT 结构内容中的密码机制来提供。这些密码机制处理的结果形成了 AUTACK 的报文体，并由相关数据(如所用的加密方法的参考、EDIFACT 结构的参考号以及原始结构的日期和时间)补充。

AUTACK 报文应使用标准的安全头段组和安全尾段组。

AUTACK 报文适用于一个或多个交换中的一个或多个报文、包或组，或者适用于一个或多个交换。

4.3.1 鉴别功能的 AUTACK 的用法

用作鉴别报文的 AUTACK 报文应由一个或多个其他 EDIFACT 结构的发送方或通过有权代表发送方行为的一方来发送。其目的是简化 GB/T 14805.5 中所定义的安全服务，即相关 EDIFACT 结构的真实性、完整性和源抗抵赖性。

AUTACK 鉴别报文能够以两种方法实现。第一种方法是传输参考的 EDIFACT 结构的散列值，该结构是由 AUTACK 自身进行安全处理的；第二种方法是用 AUTACK 只传输参考的 EDIFACT 结构的数字签名。

4.3.1.1 使用参考的 EDIFACT 结构的散列值的鉴别

经安全处理的 EDIFACT 结构应在 USX 段(安全参考)出现时参考。对于每个 USX 将至少出现一个相对应的 USY 段(参考的安全)，它包括参考的 EDIFACT 结构实施安全功能的安全结果，例如散列值。

所实施的安全功能细目将包含在这个 AUTACK 的安全头段组中。用于参考的 EDIFACT 结构的 USY 和 USH 段将通过使用两个段中的数据元安全参考号来链接。

最后一步，在 AUTACK 中传输的所有信息将通过至少使用一对安全头段组和安全尾段组加以安全处理。

注：AUTACK 使用 USX 段来引用一个或多个交换中的一个或多个报文，包或组，或者参考一个完整的交换。对于每一个 USX 段，相应的 USY 段包含应用于参考的 EDIFACT 结构的散列结果、鉴别及抗抵赖方法。

4.3.1.2 使用参考的 EDIFACT 结构的数字签名的鉴别

经安全处理的 EDIFACT 结构应在 USX 段(安全参考)出现时被引用。对于每一个 USX 段，至少应出现一个相对应的 USY 段(参考的安全性)，且该段包含参考的 EDIFACT 结构的数字签名。关于所执行的安全功能细目应包含于本 AUTACK 安全头段组中。由于可对单个参考的 EDIFACT 结构进行多次安全处理，所以应通过在这两个段中使用数据元安全控制参考号将有关的 USY 段和安全头段组链接起来。

如果参考的 EDIFACT 结构的数字签名包含于 AUTACK(而不是一个散列值)中，则 AUTACK 报文本身不需要进行安全处理。

4.3.2 确认功能的 AUTACK 的用法

用作确认报文的 AUTACK 报文应由已接收一个或多个经安全处理过的 EDIFACT 结构的接收方发送，或由有权代表接收方的一方发送。它的目的是简化对相关的 EDIFACT 结构实现接收确认、内容完整性的确认、完整性确认及接收的抗抵赖性。

确认功能只适用于经安全处理的 EDIFACT 结构。这个经安全处理过的 EDIFACT 结构应在一个 USX 段(安全参考)出现时参考。对于每一个 USX 来说,至少应出现一个相应的 USY 段。该 USY 段或者包含散列值,或者包含参考的 EDIFACT 结构的数字签名。通过使用数据元安全参考号应将 USY 段与参考的 EDIFACT 结构的安全头段组或与对 EDIFACT 结构进行安全处理的 AUTACK 报文的安全头段组链接起来。这个与参考的 EDIFACT 结构相对应的安全头包括了由原始报文的发送方对参考的 EDIFACT 结构实施的安全功能细目。

作为产生确认报文的最后一步,在 AUTACK 中传输的所有信息应由至少一对安全头段组和安全尾段组来进行安全处理。

在安全验证失败时,AUTACK 也用于非确认功能。

注:安全确认仅对经过安全处理的 EDIFACT 结构有意义。对 EDIFACT 结构进行安全处理是通过集成的安全段组(参见 GB/T 14805.5)或通过 AUTACK 鉴别来实现的。

为了避免无穷循环,用于确认功能的 AUTACK 不应要求其接收方发回 AUTACK 确认报文。

4.4 报文定义

4.4.1 数据段说明

0010 UNH,报文头

开始并唯一标识报文的服务段。

安全鉴别和确认报文的报文类型代码为 AUTACK。

数据元报文类型子功能标识用来指明 AUTACK 功能的用法,如鉴别、确认或确认的拒绝。

注:符合本标准的报文必须在 UNH 段和复合数据元 S009 中包含下列数据:

数据元	0065	AUTACK
	0052	4
	0054	1
	0051	UN

0020 段组 1:USH-USA-SG2(安全头段组)

本段组标识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(见 GB/T 14805.5的定义)。

本段组应规定应用于 AUTACK 报文或参考的 EDIFACT 结构的安全服务和算法。每个安全头段组应与一个安全尾段组相链接,并且某些安全头段组可以另外与 USY 段相链接。

0030 USH,安全头

本段规定了应用于包含本段的报文/包,或应用于参考的 EDIFACT 结构的安全服务(见 GB/T 14805.5 的定义)。

安全服务数据元应规定 AUTACK 报文或参考的 EDIFACT 结构所采用的安全服务:

——报文源鉴别和源抗抵赖性安全服务仅适用于 AUTACK 报文本身。

——参考的 EDIFACT 结构完整性、参考的 EDIFACT 结构源鉴别和参考的 EDIFACT 结构源抗抵赖性等安全服务只能由发送方用来对 AUTACK 参考的 EDIFACT 结构进行安全处理。

——接收鉴别和接收的抗抵赖性安全服务只能由经安全处理的 EDIFACT 结构的接收方对确认进行安全处理。

应按照 GB/T 14805.5 中的有关规定说明安全服务的安全应用范围。在一个 AUTACK 报文中,允许有四种安全应用范围:

——前两种范围见 GB/T 14805.5 的定义

——第三种范围包括全部 EDIFACT 结构，其中安全应用范围是从参考的报文、包、组或交换的第一个字符(即“U”)开始到报文、包、组或交换的最后一个字符为止。

——第四种范围是用户定义，即安全应用在发送方与接收方之间的协议中定义。

0040 USA，安全算法

本段标识了安全算法及由该算法所产生的技术用法，并包含了所需的技术参数(见 GB/T 14805.5的定义)。

0050 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报文/包的安全方法所需的数据(见 GB/T 14805.5 的定义)。

0060 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(见 GB/T 14805.5 的定义)。

0070 USA，安全算法

本段标识了安全算法及由该算法所产生的技术用法，并包含了所需的技术参数(见 GB/T 14805.5 的定义)。

0080 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 的定义)。

0090 USB，经安全处理的数据标识

本段应包含交换发送方和交换接收方的标识及与这个 AUTACK 安全性有关的时间标记，并且它应规定是否需要来自这个 AUTACK 报文接收方的一个安全确认。如果要求，这个报文发送方将希望得到一个报文接收方发送回来的 AUTACK 确认报文。

在 USB 中的交换发送方和交换接收方应该参考出现 AUTACK 的交换中的发送方和接收方，以便保证这个信息的安全性。

0100 段组 3：USX-USY

本段组用来标识安全进程中的参与方，并提供有关参考的 EDIFACT 结构的安全信息。

0110 USX，安全参考

本段应包含安全进程中所涉及的参与方的参考。

复合数据元安全日期和时间可以包含参考的 EDIFACT 结构的最初生成日期和时间。

如果只出现数据元 0020，而没有 0048、0062 和 0800，则参考整个交换。

如果出现数据元 0020 和 0048，而没有出现 0062 和 0800，则参考该组。

0120 USY，参考的安全

本段包含一个与安全头段组的链接，和按照被链接的安全头段组中所规定的安全服务应用于参考 EDIFACT 结构的结果。

当通过相同的安全服务并采用相同的安全参数对多个参考的 EDIFACT 结构进行安全处理时，多个 USY 段可以与相同的安全头段相链接。在这种情况下，安全头段组和相关多个 USY 之间的链接值应是相同的。

当 AUTACK 用于确认功能时，相应的安全头段组应是参考的 EDIFACT 结构的安全头段组，或者是用于向参考的 EDIFACT 结构提供鉴别功能的 AUTACK 报文的安全头段组。

在一个 USY 段中数据元 0534 的值应与以下两种情况相对应的 USH 段中 0534 的值完全相同：

——如果使用鉴别功能，就是当前的 AUTACK(安全服务：参考的 EDIFACT 结构的真实性、参考的 EDIFACT 结构的完整性或参考的 EDIFACT 结构的源抗抵赖性)。

——如果使用确认功能，就是参考的 EDIFACT 结构本身，或者向参考的 EDFIACT 结构提供鉴别功能的 AUTACK 报文(安全服务：接收的抗抵赖性或接收鉴别)。

0130 **段组** 4:UST-USR(**安全尾段组**)

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(**见** GB/T 14805.5 **的定义**)。

如果安全尾段组与某个参考的 EDIFACT **结构相关的安全头段组相链接,则** USR **段可以被省略。在这种情况下,相应的安全功能结果应能在链接到相应安全头段组的** USY **段中找到**。

0140 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,并说明包含在这些组中的安全段的数目(**见** GB/T 14805.5 **的定义**)。

0150 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进行规定的(**见** GB/T 14805.5 **的定义**)。**在这个段中,安全结果应适用于** AUTACK **报文本身**。

0160 UNT,**报文尾**

本服务段终止一个报文,并给出段的总数和报文的控制参考号。

4.4.2 报文结构

4.4.2.1 段表

位置	标记	名称	状态	最大次数	备注
0010	UNH	**报文头**	M	1	
0020	·····	**段组** 1 ———	M	99	
0030	USH	**安全头**	M	1	
0040	USA	**安全算法**	C	3	
0050	·····	**段组** 2 ———	C	2	
0060	USC	**证书**	M	1	
0070	USA	**安全算法**	C	3	
0080	USR	**安全结果**	C	1	
0090	USB	**经安全处理的数据标识**	M	1	
0100	·····	**段组** 3 ———	M	9999	
0110	USX	**安全参考**	M	1	
0120	USY	**参考的安全**	M	9	
0130	·····	**段组** 4 ———	M	99	
0140	UST	**安全尾**	M	1	
0150	USR	**安全结果**	C	1	
0160	UNT	**报文尾**	M	1	

注:AUTACK **报文的报文体由** USB **段和段组** 3 **构成**。

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。

A1.3 按段标记字母顺序排列的段索引

标记	名　称
UNH	报文头（Message header）
UNT	报文尾（Message trailer）
USA	安全算法（Security algorithm）

USB **经安全处理的数据标识**(Secured data identification)
USC **证书**(Certificate)
USH **安全头**(Security header)
USR **安全结果**(Security result)
UST **安全尾**(Security trailer)
USX **安全参考**(Security references)
USY **参考的安全**(Security on references)

A1.4 按英文名称的字母顺序排列的段索引

标记	名　称
USC	**证书**(Certificate)
UNH	**报文头**(Message header)
UNT	**报文尾**(Message trailer)
USB	**经安全处理的数据标识**(Secured data identification)
USA	**安全算法**(Security algorithm)
USH	**安全头**(Security header)
USY	**参考的安全**(Security on references)
USX	**安全参考**(Security references)
USR	**安全结果**(Security result)
UST	**安全尾**(Security trailer)

A1.5 段规范

注：在此只包含 GB/T 14805 其他部分中未定义的段。

USB **经安全处理的数据标识**

功能：包含与 AUTACK 相关的细目。

位置	标记	名称	状态	最大次数	表示	注
010	0503	**应答类型，代码型**	M	1	an..3	
020	S501	**安全日期与时间**	C	1		
	0517	**日期与时间限定符**	M		an..3	
	0338	**事件日期**	C		n..8	
	0314	**事件时间**	C		an..15	
	0336	**时差**	C		n4	
030	S002	**交换发送方**	M	1		
	0004	**交换发送方标识**	M		an..35	
	0007	**标识代码限定符**	C		an..4	
	0008	**交换发送方内部标识**	C		an..35	
	0042	**交换发送方内部子标识**	C		an..35	
040	S003	**交换接收方**	M	1		
	0010	**交换接收方标识**	M		an..35	
	0007	**标识代码限定符**	C		an..4	
	0014	**交换接收方内部标识**	C		an..35	

	0046	交换接收方内部子标识	C		an..35	

USX 安全参考

功能:参照经安全处理的 EDIFACT 结构及其有关的日期和时间。

位置	标记	名称	状态	最大次数	表示	注
010	0020	交换控制参考	C	1	an..14	
020	S002	交换发送方	C	1		
	0004	交换发送方标识	M		an..35	
	0007	标识代码限定符	C		an..4	
	0008	交换发送方内部标识	C		an..35	
	0042	交换发送方内部子标识	C		an..35	
030	S003	交换接收方	C	1		
	0010	交换接收方标识	M		an..35	
	0007	标识代码限定符	C		an..4	
	0014	交换接收方内部标识	C		an..35	
	0046	交换接收方内部子标识	C		an..35	
040	0048	段组参考号	C	1	an..14	1,3
050	S006	应用发送方标识	C	1		1
	0040	应用发送方标识	M		an..35	
	0007	标识代码限定符	C		an..4	
060	S007	应用接收方标识	C	1		3
	0044	应用接收方标识	M		an..35	
	0007	标识代码限定符	C		an..4	
070	0062	报文参考号	C	1	an..14	2,4
080	S009	报文标识符	C	1		4
	0065	报文类型	M		an..6	
	0052	报文版本号	M		an..3	
	0054	报文发布号	M		an..3	
	0051	管理机构,代码型	M		an..3	
	0057	机构指定的代码	C		an..6	
	0110	代码列表目录版本号	C		an..6	
	0113	报文类型子功能标识	C		an..6	
090	0800	包参考号	C		an..6	2
100	S501	安全日期与时间	C	1		

0517	日期与时间限定符	M	an..3
0338	事件日期	C	n..8
0314	事件时间	C	an..15
0336	时差	C	n4

从属性注释：

1 D5(050,040) 如果第一项有，则全有。

2 D1(070,090) 有一项且仅有一项。

3 D5(060,040) 如果第一项有，则全有。

4 D5(080,070) 如果第一项有，则全有。

USY 参考的安全

功能：标识适用的头，并包含安全结果和/或指明导致安全错误原因的参考值。

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	
020	S508	确认结果	C	2		1
	0563	确认值限定符	M		an..3	
	0560	确认值	C		an..512	
030	0571	安全错误，代码型	C	1	an..3	1

注：1 D3(020,030) 有一项或多项

A2 复合数据元目录

未定义复合数据元。

A3 简单数据元目录

A3.1 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。

注：简单数据元注号。

A3.2 按标记排列的简单数据元索引

标记	名称
0020	交换控制参考(Interchange control reference)
0048	组参考号(Group reference number)
0062	报文参考号(Message reference number)
0503	应答类型,代码型(Response type,coded)
0534	安全参考号(Security reference number)
0571	安全错误,代码型(Security error,coded)
0800	包参考号(Package reference number)

A3.3 按英文名称的字母顺序排列的简单数据元索引

标记	名称
0048	组参考号(Group reference number)
0020	交换控制参考(Interchange control reference)
0062	报文参考号(Message reference number)
0800	包参考号(Package reference number)
0503	应答类型,代码型(Response type,coded)
0571	安全错误,代码型(Security error,coded)
0534	安全参考号(Security reference number)

A3.4 简单数据元说明

注:在此只包含 GB/T 14805 其他部分未定义的简单数据元。

0571 安全错误,代码型

描述:标识导致拒绝 EDIFACT 结构的安全错误。

表示:an..3

注:此数据元应说明所出现的安全错误。这些错误可能是导致对安全确认请求的未确认,或者可以是一个包含错误的 AUTACK,或经安全处理的 EDIFACT 结构的接收方主动发送的。

附 录 B
(提示的附录)
服务代码目录

服务代码目录由 UN/ECE 维护并且是联合国贸易数据交换目录(UNTDID)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。

附 录 C
(提示的附录)
AUTACK 报文示例

在此提供三个示例来解释 AUTACK 报文的不同应用。

第一个示例说明了在提供源抗抵赖性的安全服务时,如何使用 AUTACK 报文来保护前面发送的报文。这需要 AUTACK 确认报文。

第二个示例说明了一个 AUTACK 报文如何用不同安全服务来保护两个报文:一个报文发起方的抗抵赖,对另一个报文的源鉴别。

第三个示例解释了用于安全确认的 AUTACK 报文的用法。它说明了在第一个示例中由 AUTACK 报文所要求的 AUTACK 确认报文。

C1 示例 1:由一个 AUTACK 报文提供的源抗抵赖性的服务

C1.1 概述

当付款通知报文超过一定数量时,A 银行需要由 A 公司的 Smith 先生来对 A 公司的付款通知报文实施源抗抵赖性的安全服务。

双方间的交换协定规定了 A 银行所要求的源抗抵赖性安全服务应由 A 公司的 Smith 先生用数字签名的方式对这些付款通知报文实施加密来完成。

双方都同意这个数字签名是通过 512 位 RSA(非对称算法)对由 MD5 算法算出的散列值进行计算生成的。

标识 Smith 先生公开密钥的证书由双方都信任的 AUTHORITY 机构(即证书的发布者)发布。

在这些条件下,由于 PAYORD(付款通知报文)的数字签名被包含在 AUTACK 报文中,因此 AUTACK 本身不需要被签名。

由 AUTACK 保护的 PAYORD 报文是 Smith 先生发给 A 银行首次交换中的第三个报文。它于 1996 年 1 月 15 日 10:00 生成。

该 AUTACK 本身是交换中的第五个报文,它由 1996 年 1 月 15 日 10:5:32 生成。出现的安全段如下:

——指示对 PAYORD 报文应用安全服务的 USH 段;

——USC-USA-USA-USA-USR,Smith 先生的证书;

——USB;

——带有(PAYORD 报文的)安全参考和安全结果的 USX-USY;

——UST,没有 USR,参考 USH。

C1.2 安全细目

安全头	
安全服务,代码型	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:1
过滤函数	用十六进制的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—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
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 证书的发布者 密钥名称	 Smith 先生的证书由认证机构 AUTHORITY 生成 用于生成 Smith 证书的 AUTHORITY 公共密钥是 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

表(续)

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	计算签名时所用的服务字符 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	计算签名时所用的服务字符 服务字符是数据元分隔符 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	计算签名时所用的服务字符 服务字符是复合数据元分隔符 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	计算签名时所用的服务字符 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	计算签名时所用的服务字符 服务字符是释放分隔符 值“?”(问号)
安全日期与时间 日期与时间	证书生成时间 Smith 先生证书于 93 年 12 月 15 日 14：12：00 生成
安全日期与时间 日期与时间	证书有效期的生效时间 Smith 先生证书有效期的开始时间是： 1996 01 01　00：00：00
安全日期与时间 日期与时间	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	由 Smith 先生用于签名的非对称算法
安全算法 算法的使用 密码操作方式 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 先生模数的长度(位数) Smith 先生模数的长度为 512 位
安全算法	由 AUTHORITY 用于生成 Smith 先生证书的散列函数
安全算法 算法的使用 密码操作方式 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》)来提供一个双倍长的散列代码(128 位)；初始化值： A＝01234567　　B＝89ABCDEF C＝FEDCBA98　　D＝76543210 使用 MD5 报文—文摘算法

表(完)

安全算法	AUTHORITY 用于签名的非对称算法
安全算法 算法的使用 密码操作方式 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 AUTHORITY 模数的长度(位数) AUTHORITY 模数的长度是 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 位过滤的十六进制数字签名
经安全处理的数据标识	
应答类型,代码型	需要一个来自 A 银行的安全确认
安全日期与时间	AUTACK 的安全时间标记是:1996 01 15　10:05:32
交换发送方 交换发送方标识	交换发送方的标识 A 公司 Smith 先生的标识
交换接收方 交换接收方标识	交换接收方的标识 A 银行的标识
安全参考	涉及安全实体(具有源抗抵赖性服务相关的 PAYORD)及其相应日期和时间
交换控制参考	标识发送方分配给 PAYORD 报文交换的参考号:1
交换发送方 交换发送方标识	 标识 PAYORD 报文交换的发送方是:A 公司的 Smith 先生
交换接收方 交换接收方标识	 标识 PAYORD 报文交换的接收方是:A 银行
报文参考号	标识发送方分配给 PAYORD 报文的参考号:3
安全日期与时间 日期和时间	参考 PAYORD 的安全时间标记 这个安全时间标记是:日期为 1996 01 15　时间为 10:00:00
参考的安全	标识可用的安全头(涉及 PAYORD 报文所应用的安全功能)和 PAYORD 报文应用这些功能后的结果
安全参考号	将确认结果同相应的 USH 段连接起来的参考号。在本例中,该值为 1
确认结果 确认值限定符 确认值	 (PAYORD 报文的)数字签名 512 位过滤的十六进制数字签名
安全尾	
安全参考号	该安全尾的参考号是 1
安全段数	安全段数为 7

C2 示例 2:用 AUTACK 保护多个报文

C2.1 概述

当付款通知报文超过一定数量时,A 银行需要由 A 公司的 Smith 先生来对 A 公司的付款通知报文实施源抗抵赖性的安全服务。对于那些未超出该数量的付款通知报文,则需要报文源鉴别功能。

双方间的交换协定规定了 A 银行所要求的源抗抵赖性安全服务应由 A 公司的 Smith 先生用数字签名的方式对这些付款通知报文实施加密来完成。

双方都同意这个数字签名是通过 512 位 RSA(非对称算法)对由 MD5 算法算出的散列值进行计算生成的。

此外,报文的源鉴别将在发送方端按照 ISO 8731-1 通过使用对称的 DES 算法生成一个"报文鉴别码"(MAC)来实现。

标识 Smith 先生公开密钥的证书由双方都信任的 AUTHORITY 机构(即证书的发布者)发布。

发送的第一个 PAYORD 报文必须通过 AUTACK 用数字签名方式加以保护。这个 PAYORD 报文是 Smith 先生发给 A 银行首次交换中的第五个报文。它是在 1996 年 1 月 15 日 08:00:00 发送的。

发送的第二个 PAYORD 报文必须通过 AUTACK 用 MAC 方式加以保护。它是首次交换中的第七个报文,于 1996 年 1 月 15 日 09:00:00 发送。

AUTACK 报文本身是首次交换中的第十个报文。它是在 1996 年 1 月 15 日 10:05:32 发送的。

由于第一个 PAYORD 报文是用数字签名方式加以保护的,AUTACK 本身不需要被签名。

因此,所出现的安全段如下:

——指示对第一个 PAYORD 报文应用源抗抵赖性服务的 USH 段

——USC-USA-USA-USA-USR,Smith 先生的证书。

——指示对第二个 PAYORD 报文应用报文源鉴别服务的 USH 段

——USB

——带有第一个 PAYORD 报文安全参考和安全结果(数字签名)的 USX-USY

——带有第二个 PAYORD 报文安全参考和安全结果(MAC)的 USX-USY

——UST,没有 USR,参考第一个 USH。

——UST,没有 USR,参考第二个 USH。

C2.2 安全细目

安全头	安全头包括了对所参考的实体(即第一个 PAYORD 报文)实施安全功能的信息
安全服务,代码型	第一个 PAYORD 报文的源抗抵赖性
安全参考号	本安全头的参考号是 1
过滤函数	用十六进制过滤器过滤所有二进制的值(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	A 公司的 Smith 先生
安全标识细目 报文接收方	A 银行
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

表(续)

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 证书的 AUTHORITY 公共密钥是 PK1
证书语法版本	UN/EDIFACT 服务段目录的证书版本
过滤函数	用十六进制过滤器过滤所有二进制值(密钥和数字签名)
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	计算签名时所用的服务字符 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	计算签名时所用的服务字符 服务字符是数据元分隔符 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	计算签名时所用的服务字符 服务字符是复合数据元分隔符 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	计算签名时所用的服务字符 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	计算签名时所用的服务字符 服务字符是释放分隔符 值“?”(问号)
安全日期和时间 日期和时间	证书生成时间 Smith 先生证书于 93 年 12 月 15 日　14：12：00 生成的
安全日期和时间 日期和时间	证书有效期的生效时间 Smith 先生证书有效期的开始时间是： 1996 01 01　00：00：00
安全日期和时间 日期和时间	证书有效期的结止时间 Smith 先生证书有效期结止时间是： 1996 12 31　23：59：59
安全算法	由 Smith 先生用于签名的非对称算法
安全算法 算法的使用 密码操作方式 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 先生模数的长度(位数) Smith 先生模数的长度为 512 位
安全算法	由 AUTHORITY 用于生成 Smith 先生证书的散列函数

表(续)

安全算法 算法的使用 密码操作方式 算法	 使用发布者散列算法 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》)来提供一个双倍长的散列代码(128 位);初始化值: A=01234567　　B=89ABCDEF C=FEDCBA98　　D=76543210 使用 MD5 报文—文摘算法
安全算法	AUTHORITY 用于签名的非对称算法
安全算法 算法的使用 密码操作方式 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 AUTHORITY 模数的长度(位数) AUTHORITY 模数的长度是 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 位过滤的十六进制数字签名
安全头	安全头包括了对所参考的实体(即第二个 PAYORD 报文)实施安全功能的信息
安全服务,代码型	第二个 PAYORD 的报文源鉴别
安全参考号	本安全头的参考号是 2
过滤函数	用十六进制过滤器过滤所有二进制值
安全标识细目 报文发送方	 A 公司的 Smith 先生
安全标识细目 报文接收方	 A 银行
安全算法	
安全算法 算法的使用 密码操作方式 算法	 使用对称算法来实现报文的源鉴别 按照 ISO 8731-1,计算一个 MAC 使用 DES 算法
算法参数 算法参数限定符 算法参数值	 标识本算法参数值为以前交换的对称密钥的名称
经安全处理的数据标识	
应答类型,代码型	不需要来自 A 银行的确认

表(完)

安全日期与时间	AUTACK 安全时间标记 该安全时间标记为:日期:1996 01 15 时间:10:05:32
交换发送方 交换发送方标识	交换发送方的标识 A 公司 Smith 先生的标识
交换接收方 交换接收方标识	交换接收方的标识 A 银行的标识
安全参考	涉及的安全实体(即第二个 PAYORD 报文)
交换控制参考	标识发送方分配给第二个 PAYORD 报文交换的参考号:1
交换发送方 交换发送方标识	标识 PAYORD 报文交换的发送方:即 A 公司的 Smith 先生
交换接收方 交换接收方标识	标识 PAYORD 报文交换的接收方:即 A 银行
报文参考号	标识发送方分配给第二个 PAYORD 报文的参考号:7
安全日期与时间	本安全时间标记是:日期:1996 01 15　时间:9:00:00
参考的安全	标识可用的安全头(涉及第二个 PAYORD 报文所应用的安全功能)和该报文应用这些功能后的结果
安全参考号	将确认结果同相应的 USH 段连接起来的参考号。在本例中,该值为 2
确认结果 确认值限定符 确认值	 MAC(报文鉴别码)
安全参考	涉及安全实体(第一个 PAYORD 报文)及其相应日期和时间
交换控制参考	标识发送方分配给 PAYORD 报文交换的参考号:1
交换发送方 交换发送方标识	标识 PAYORD 报文交换的发送方:A 公司的 Smith 先生
交换接收方 交换接收方标识	标识 PAYORD 报文交换的接收方:A 银行
报文参考号	标识发送方分配给 PAYORD 报文的参考号:5
安全日期与时间	本安全时间标记是:日期为 1996 01 15　时间为 10:00:00
参考的安全	标识可用的安全头(涉及对第一个 PAYORD 报文所应用的安全功能)和该报文应用这些功能后的结果
安全参考号	将确认结果同相应的 USH 段连接起来的参考号。在本例中,该值为 1
确认结果 确认值限定符 确认值	 (第一个 PAYORD 报文的)数字签名 512 位过滤的十六进制数字签名
安全尾	
安全参考号	本安全尾的参考号是 2
安全段数	安全段数为 2
安全尾	
安全参考号	这个安全尾的参考号是 1
安全段数	安全段数为 7

C3 示例 3:通过 AUTACK 报文实现接收报文的安全确认

C3.1 概述

在示例 1 中,AUTACK 由先前的 PAYORD 报文的发送方(A 公司的 Smith 先生)使用。该 AUTACK 报文要求 A 银行给予确认。

本例将说明如何用 AUTACK 报文进行安全确认。

作为安全确认的 AUTACK 报文将通过采用数字签名方式的源抗抵赖性安全服务加以保护,并且这些工作已经完成。

该 AUTACK 报文生成于 1996 年 1 月 16 日 11:00,是交换中的第二十个报文。

出现的安全段如下:

——USH,标识 AUTACK 报文所应用的安全服务;

——USH,标识确认的实体所应用的安全服务;

——USC-USA(3)-USR,A 银行的证书;

——USB,包括 AUTACK 的详细内容;

——USX-USY,包括确认实体的参考和数字签名;

——UST,没有 USR 的安全尾;

——UST-USR,保护 AUTACK 报文本身。

C3.2 安全细目

安全头	
安全服务,代码型	源抗抵赖性
安全参考号	本安全头的参考号是 1
过滤函数	用十六进制过滤器过滤所有二进制值
源字符集编码	当生成 MAC 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(产生数字签名的一方)	 A 银行
安全标识细目 报文接收方(验证数字签名的一方)	 A 公司的 Smith 先生
安全顺序号	本报文的安全顺序号是 20
安全日期和时间	该安全时间标记是:日期:1996 01 16　时间:11:00
证书	A 银行的证书
证书参考	本证书由 AUTHORITY 参考:00000010
安全标识细目 证书持有者	 A 银行
安全标识细目 证书发布者 密钥名称	 A 银行的证书由认证机构 AUTHORITY 生成 用于生成 A 银行证书的 AUTHORITY 的公共密钥是 PK1
证书语法版本	UN/EDIFACT 服务段目录的证书版本
过滤函数	用十六进制过滤器过滤所有二进制值(密钥和数字签名)
源字符集编码	当生成证书时,证书凭证用 GB/T 1988(即 ASCII 码)8 位进行编码

表(续)

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	计算签名时所用的服务字符 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	计算签名时所用的服务字符 服务字符是数据元分隔符 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	计算签名时所用的服务字符 服务字符是复合数据元分隔符 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	计算签名时所用的服务字符 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	计算签名时所用的服务字符 服务字符是释放分隔符 值“?”(问号)
安全日期和时间 日期和时间	证书生成时间 A 银行的证书生成于 1995 12 31　14：00：00
安全日期和时间 日期和时间	证书有效期的生效时间 A 银行证书有效期的开始时间为：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 A 银行证书有效期的截止时间为：1996 12 31　23：59：59
安全算法	由 A 银行用于签名的非对称算法
安全算法 算法的使用 密码操作方式 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 A 银行的公开密钥
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 A 银行的模数
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 先生模数的长度(位数) A 银行模数的长度为 512 位
安全算法	由 AUTHORITY 用于生成 A 银行证书的散列函数
安全算法 算法的使用 密码操作方式 算法	 使用发布者散列算法 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》)来提供一个双倍长的散列代码(128 位)；初始化值： A＝01234567　B＝89ABCDEF C＝FEDCBA98　D＝76543210 使用 MD5 报文-文摘算法
安全算法	AUTHORITY 用于签名的非对称算法

表(续)

安全算法 算法的使用 密码操作方式 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 AUTHORITY 模数的长度(位数) AUTHORITY 模数的长度是 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 位过滤的十六进制数字签名
安全头	安全头包括了对所参考的实体(即 PAYORD 报文)实施安全功能的信息
安全服务,代码	源抗抵赖性
安全参考号	本安全头的参考号是 2
过滤函数	用十六进制过滤器过滤所有二进制值(签名)
源字符集编码	当生成报文签名时,该报文用 GB/T 1988(即 ASCII 码)8 位进行编码
经安全处理的数据标识	
安全日期和时间	该 AUTACK 报文的安全时间标记是:日期:1996 01 16 时间:11:00
交换发送方 交换发送方标识	交换发送方的标识 A 银行的标识
交换接收方 交换接收方标识	标识交换接收方 A 公司 Smith 先生的标识
安全参考	涉及安全实体(确认的报文)及其相关的日期和时间
交换控制参考	标识确认的 PAYORD 报文交换的参考号是:1
交换发送方 交换发送方标识	 标识确认的报文所属交换的发送方:A 公司的 Smith 先生
交换接收方 交换接收方标识	 标识确认的报文交换的接收方:A 银行
报文参考号	标识由发送方分配给确认的报文的参考号:3(见例 1)
安全日期与时间	该 PAYORD 的安全时间标记是:日期:1996 01 15　时间:10:00:00
参考的安全	
安全参考号	标识可应用的头 2

表(完)

确认结果 确认值限定符 确认值	 确认的 PAYORD 报文的数字签名 512 位过滤的十六进制数字签名
安全尾	
安全参考号	该安全尾的参考号是 2
安全段数	安全段数为 3
安全尾	
安全参考号	这个安全尾的参考号是 1
安全段数	安全段数为 7
安全结果	
确认结果 确认值限定符 确认值	 AUTACK 的数字签名 512 位过滤的十六进制数字签名

附 录 D
(提示的附录)
安全服务及算法

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,便向他提供一个基点以得到适合其特定应用的解决方案。

为便于阅读和理解,本主题被分为三个部分。每个部分针对了应用安全的不同原则。

这三个部分是:

a) 采用对称算法和参考实体的 AUTACK 报文的组合。

b) 采用非对称算法和参考实体的 AUTACK 报文的组合。

c) 采用确认 AUTACK 报文的组合。

各表中使用的代码清单(完整代码表的子集)

0501 安全服务,代码型
- 1 源抗抵赖性
- 2 报文的源鉴别
- 9 参考的 EDIFACT 结构的完整性

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

0505 过滤函数,代码型
- 6 UN/EDIFACT EDC 过滤器

0525 密码操作方式,代码型
- 6 MAC(报文鉴别码)
- 9 MDC2(修改检查码)
- 11 HDS2(散列功能)

0527 算法,代码型
1 DES(数据加密标准)
10 RSA(Rivest,Shamir,Adleman)

0531 算法参数限定符
12 模数
13 指数
14 模数长度

0563 确认值限定符
1 唯一的确认值

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

使用的缩写

a,b,c,d	=	安全参考号的表示法
CA	=	认证机构
Enc-Key	=	加密密钥
Hash	=	散列值
Key-N	=	密钥名称
MAC	=	报文鉴别码
Mod	=	模数
Mod-L	=	模数长度
PK/CA	=	认证机构的公开密钥
Pub-K	=	公开密钥
Sig	=	签名

D2 采用对称算法和参考实体 AUTACK 报文的组合

表 D1 为下列特定情况建立了的关系:

——由 AUTACK 报文向参考的实体提供保护。

——只使用对称算法。

——提供的安全服务是对于参考报文的参考 EDIFACT 结构的源鉴别和 AUTACK 报文的报文源鉴别。参考的 EDIFACT 结构源鉴别是通过参考的 EDIFACT 结构完整性和 AUTACK 的报文源鉴别的组合来提供的。

——参考的 EDIFACT 结构完整性是通过基于 DES 算法的散列函数来提供的,该 DES 算法按照 ISO 10118-2 采用 MDC 方式。在发送方和接收方没有共享的秘密密钥。该散列值在 AUTACK 中被传输且通过 AUTACK 报文上的安全性得以保护。

——AUTACK 的报文源鉴别是通过对 AUTACK 报文计算一个 MAC(报文鉴别码)来提供的。在本例中,所用的算法是使用秘密密钥的 CBC 方式的 DES,该秘密密钥为报文接收方所知且只通过密钥名称来引用。本示例符合 ISO 8731-1。

——尽管发送方和接收方共享密钥,但是密码机制事先并未达成完全一致。因此,所用的全部算法和操作方式要被明确地指定。

——在此仅列出与实际使用的安全技术、算法和操作方式相关的安全段。

表 D1 当只采用对称算法时的关系矩阵

标记	名 称	状态	最大次数	参考的 EDIFACT 结构完整性 ISO 10118-2	AUTACK 报文源鉴别 ISO 8731-1	注
SG1		M	99	每个安全服务 1 个		
USH	安全头	M	1			
0501	安全服务,代码型	M		9	2	
0534	安全参考号	M		a	b	1
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	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	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	2	
0525	密码操作方式,代码型	C		9/*	6/*	
0527	算法,代码型	C		1/*	1/*	
USB	经安全处理的数据标识	M	1	经安全处理的数据结构的参考		
SG3		M	9999			
USX	安全参考	M	1			
USY	参考的安全	M	9			
0534	安全参考号	M		a	—	5
S508	确认结果	C	2			
0563	确认值限定符	M		1		
0560	确认值	C		Hash		6
SG4		M	99			
UST	安全尾	M	1			
0534	安全参考号	M		a	b	7
0588	安全段数	M				
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			MAC	8

表 D1(完)

标记	名　　称	状态	最大次数	参考的EDIFACT结构完整性 ISO 10118-2	AUTACK报文源鉴别 ISO 8731-1	注
注 1　一个安全头参照 AUTACK 的安全尾,其他的安全头则参照"参考的安全"段。 2　报文发送方。 3　AUTACK 报文的发送方和接收方共享的秘密密钥名称。 4　报文接收方。 5　参照安全头之一。 6　对参考的 EDIFACT 结构计算出的散列值。该值由 AUTACK 报文计算出的 MAC 来保护。 7　参照安全头之一。 8　对 AUTACK 报文计算出的 MAC。 *　进一步的代码组合是可能的和需要的。						

D3　采用非对称算法和参考实体的 AUTACK 报文的组合

表 D2 为下列特定情况建立了的关系:

——由 AUTACK 报文向参考的实体提供保护。

——只使用对称算法。

——提供的安全服务是对于参考报文的参考 EDIFACT 结构的源抗抵赖性和 AUTACK 报文的报文源抗抵赖性。参考的 EDIFACT 结构源抗抵赖性是通过参考的 EDIFACT 结构完整性和 AUTACK 的报文源抗抵赖性的组合来提供的。

——非对称算法是 RSA。

——散列函数是 MDC 方式的 DES 算法。相同的散列函数用来计算参考的 EDIFACT 结构的散列值和 AUTACK 报文的散列值。

——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。

——只包含一个证书,仅当使用接收方的公开密钥时,第二个证书才是必要的。

表 D2　使用非对称算法时的关系矩阵

标记	名　　称	状态	最大次数	参考的EDIFACT结构完整性 ISO 10118-2	AUTACK报文的源抗抵赖性 (RSA)	注
SG1		M	99	每个安全服务 1 个		
USH	安全头	M	1			
0501	安全服务,代码型	M		9	1	1
0534	安全参考号	M		c	D	
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	2

表 D2(续)

标记	名　　称	状态	最大次数	参考的EDIFACT结构完整性ISO 10118-2	AUTACK报文的源抗抵赖性(RSA)	注
S500	安全标识细目	C	2			
0577	安全参与方限定符	M		2	2	3
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	4
0525	密码操作方式,代码型	C		9/*	9/*	
0527	算法,代码型	C		1/*	1/*	
SG2		C	2		只有一个:发送方证书	
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	5
S500	安全标识细目	C	2		(鉴别方)	
0577	安全参与方限定符	M			4	6
0538	密钥名称	C			(PK/CA 名称)	
USA	安全算法	C	3		(发送方的签名函数)	
S502	安全算法	M	1			
0523	算法的使用,代码型	M			6	7
0527	算法,代码型	C			10	
S503	算法参数	C	9		(模数长度)	
0531	算法参数限定符	M			14	
0554	算法参数值	M			Mod-L	
S503	算法参数	C	9		(模数)	
0531	算法参数限定符	M			12	
0554	算法参数值	M			模数	
S503	算法参数	C	9		(公开指数)	
0531	算法参数限定符	M			13	
0554	算法参数值	M			公共密钥	
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			

表 D2(续)

标记	名　　称	状态	最大次数	参考的 EDIFACT 结构完整性 ISO 10118-2	AUTACK 报文的源抗抵赖性 (RSA)	注
0523	算法的使用,代码型	M			4	8
0525	密码操作方式,代码型	C			11	
0527	算法,代码型	C			1	
USA	安全算法	C	3		(用于证书签名的 CA 的签名函数)	
S502	安全算法	M	1			
0523	算法的使用,代码型	M			3	9
0527	算法,代码型	C			10	
USR	安全结果	C	1			
S508	确认结果	M	2			10
0563	确认值限定符	M			1	
0560	确认值	C			Sig	
USB	经安全处理的数据标识	M	1	经安全处理的数据结构的参考		
SG3		M	9999			
USX	安全参考	M	1			
USY	参考的安全	M	9			
0534	安全参考号	M		c	—	
S508	确认结果	M	2			10
0563	确认值限定符	M		1	—	
0560	确认值	C		Hash	—	
SG4		M	99			
UST	安全尾	M	1			
0534	安全参考号	M		c	d	
USR	安全结果	C	1			
S508	确认结果	M	2			10
0563	确认值限定符	M			1	
0560	确认值	C		—	Sig	

注

1 假设 AUTACK 的报文源鉴别和完整性被包括在源抗抵赖性中。参考的 EDIFACT 结构的源抗抵赖性是通过参考的 EDIFACT 结构完整性和 AUTACK 源抗抵赖性的组合来提供的。

2 报文发送方。

3 报文接收方。

4 发送方应用于经安全处理的结构上的散列函数。

表 D2(完)

标记	名　　称	状态	最大次数	参考的 EDIFACT 结构完整性 ISO 10118-2	AUTACK 报文的源抗抵赖性 (RSA)	注
5　证书持有者:标识细目应与报文发送方 USH S500 中的相同。 6　鉴别方:认证机构(CA)。 7　发送方的签名函数。 8　CA 的散列函数。 9　CA 的签名函数。 10　某些签名算法(例如 DSA)需要两个结果参数。 *　进一步的代码组合是可能的和需要的。						

D4　采用确认 AUTACK 报文的组合

确认 AUTACK 报文的可能组合遵循以上描述的示例。

特别是:

——对于 USH 0501 的代码为 6(接收鉴别)采用表 D1 的组合;

——对于 USH 0501 的代码为 5(接收方的抗抵赖)采用表 D2 的组合。

注:进一步的代码组合是可能的和需要的。

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 6 部分：安全鉴别和确认报文
（报文类型为 AUTACK）
GB/T 14805.6—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
版权专有　不得翻印
*
开本 880×1230　1/16　印张 2　字数 58 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：155066·1-16676　定价 16.00 元
*
标 目 407—09

GB/T 14805.6-1999