ICS 35.240.40
A 11

中华人民共和国国家标准

GB/T 27929—2011

银行业务　采用对称加密技术进行报文鉴别的要求

Banking—Requirements for message authentication using symmetric techniques

(ISO 16609:2004,MOD)

2011-12-30 发布　　2012-05-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　次

前言 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　保护 …… 4
5　报文鉴别过程 …… 5
6　核准的 MAC 算法 …… 6
附录 A（规范性附录）　核准的报文鉴别用分组密码算法 …… 9
附录 B（资料性附录）　编码字符集的报文鉴别 …… 11
附录 C（资料性附录）　编码字符集报文鉴别的示例 …… 15
附录 D（资料性附录）　标准电传格式的报文鉴别框架 …… 19
附录 E（资料性附录）　使用 MID 防重复和丢失保护 …… 21
附录 F（资料性附录）　伪随机数发生器 …… 22
附录 G（资料性附录）　会话密钥导出 …… 23
附录 H（资料性附录）　一般指导信息 …… 24
参考文献 …… 25

前　言

本标准修改采用 ISO 16609:2004《银行业务　采用对称加密技术进行报文鉴别的要求》(英文版)。

本标准根据 ISO 16609:2004 重新起草,与 ISO 16609:2004 的技术性差异为:

a) 将标准原文中的"T-DEA"按照我国通常习惯修改为"3-DEA";

b) 在 A.4.1 中,将"为加入本标准而提出的可选鉴别算法应由国家标准机构提交给 ISO/TC 68,或征得国家标准机构的同意后提交给 ISO/TC 68"修改为"为加入本标准而提出的可选鉴别算法应由国家标准机构提交给国家密码相关管理部门,或征得国家标准机构的同意后提交给国家密码相关管理部门";

c) 在 A.4.4 提到算法时,将"按照 IEC/ISO 相关程序对其进行评估"修改为"按照国家相关程序对其进行评估";

d) 在 A.4.5 中,将"每个新提案应由 ISO 审查"修改为"每个新提案应由国家相关机构审查",本段中"以及提出的算法是否符合国际标准的条件及要求"修改为"以及提出的算法是否符合国内标准的条件及要求";

e) 在 A.4.7 申诉程序中,将"提案被拒绝时(见 A.4.5),若该提案尚未进行公开审核,发起人可要求 ISO/TC 68 秘书处就该提案进行公开审核(见 A.4.6)。如果已进行公开审核且仍被拒绝,则发起人可要求 TC 68 秘书处将申请连同有关审核报告的备份提交技术委员会的 P 成员进行表决,表决采用多数通过原则。循环审查该提案。其投票的简单多数通过即为最终结果"修改为"提案被拒绝时(见 A.4.5),发起人可要求国内相关机构就该提案进行审核(见 A.4.6),审核结果即为最终结果"。

为便于使用,本标准还做了下列编辑性修改:

a) 将原文中的"本国际标准"改为"本标准";

b) 删除 ISO 16609:2004 的前言,修改了 ISO 16609:2004 的引言。

本标准的附录 A 为规范性附录,附录 B～附录 H 为资料性附录。

本标准由中国人民银行提出。

本标准由全国金融标准化技术委员会(SAC/TC 180)归口。

本标准负责起草单位:中国金融电子化公司。

本标准参加起草单位:中国人民银行、中国工商银行股份有限公司、中国银行股份有限公司、交通银行股份有限公司、中国银联股份有限公司、华北计算技术研究所、北京工商大学、中国人民银行太原中心支行。

本标准主要起草人:王平娃、陆书春、李曙光、吕毅、杨颖莉、刘运、全红、林中、张启瑞、刘先、仲志晖、李彦智、周亦鹏、李劲松、钱湘隆、赵志兰、贾树辉、马小琼、景芸、刘志军、张龙龙。

引　言

报文鉴别码(MAC)是用于验证报文真实性的一个数据域。它由报文的发送方产生且与报文一起传送。通过验证 MAC,接收方能够检测报文是否被改变以及改变是由意外还是故意欺诈引起。

本标准适用于与银行业务相关的金融机构希望以安全且有利于双方互操作的方式进行报文鉴别的情况。

本标准与被替代的 ISO 8730 和 ISO 9807 中规定的要求相一致。

银行业务　采用对称加密技术进行报文鉴别的要求

1　范围

本标准规定了用于保护银行业务报文的完整性和验证报文来源的过程，该过程与所使用的传输过程无关。本标准也给出了使用分组密码进行银行业务报文鉴别的方法。此外，由于通信双方有必要采用相同的数据表示形式，因此本标准中定义了几种数据表示方法。本标准给出了已核准的计算报文鉴别码(MAC)的分组密码列表，也给出了核准附加分组密码的方法。本标准中定义的鉴别方法适用于以编码字符集和二进制形式进行格式化及传输的报文。

本标准适用于发送方和接收方采用相同密钥的对称算法，未规定生成共享密钥的方法，也未提供防止报文受到未授权泄漏的加密过程。本标准的使用不能防止发送方和接收方的内部欺诈或者接收方伪造 MAC。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

ISO 8583　产生报文的金融交易卡　交换报文规范

ISO 8732:1988　银行业务　密钥管理(批发)

ISO/IEC 9797-1:1999　信息技术　安全技术　报文鉴别码　第 1 部分:分组密码算法的使用

ISO/IEC 9797-2:2002　信息技术　安全技术　报文鉴别码　第 2 部分:哈希函数的使用

ISO/IEC 10116　信息技术　安全技术　n 比特分组密码运算模式

ISO/IEC 10118-3:1998　信息技术　安全技术　哈希函数　第 3 部分:专用哈希函数

ISO 11568-1　银行业务　密钥管理(零售)　密钥管理介绍

ISO 11568-2:1994　银行业务　密钥管理(零售)　对称密码的密钥管理技术

ISO 11568-3　银行业务　密钥管理(零售)　对称密码的密钥生命周期

ISO 13491(所有部分)　银行业务　安全加密设备(零售)

ANSI X3.92:1981　美国信息技术国家标准　数据加密算法

ANSI X9.52:1998　美国金融服务业国家标准　三重数据加密算法　工作模式

3　术语和定义

下列术语和定义适用于本文件。

3.1

算法　algorithm

用于计算的特定数学过程或规则；遵循该过程或规则，能得到规定的结果。

3.2

鉴别　authentication

在发送方和接收方之间用于保证数据完整性并提供数据源鉴别的过程。

3.3

鉴别算法 authentication algorithm

与一个鉴别密钥和一个或多个鉴别元素共同使用的用于鉴别的算法。

3.4

鉴别元素 authentication element

通过鉴别进行保护的报文元素。

3.5

鉴别密钥 authentication key

用于鉴别的密钥。

3.6

受益人 beneficiary

作为转账的结果而被贷记或被支付的最终方。

3.7

分组密码算法 block cipher

能够将固定长度比特串和保密密钥映射到具有相同固定长度的其他比特串的算法。

3.8

偏差 bias

在产生随机数或伪随机数时，某些数出现的几率大大超过其他数的情况。

3.9

密钥周期 cryptoperiod

给定的时间周期，该周期中特定的密钥被授权使用或者在此周期中给定系统中的密钥有效。

3.10

密码分析 cryptanalysis

破解密码的技术和科学。

3.11

数据完整性 data integrity

数据没有被以未授权的方式更改或破坏的特性。

3.12

计算 MAC 日期(DMC) date MAC computed (DMC)

发送方计算报文鉴别码的日期。

注：DMC 可用于通过选择合适的密钥来同步鉴别过程。

3.13

数据源鉴别 data origin authentication

确认接收到的数据源与声明一致。

3.14

解密 decipherment decryption

加密的逆过程。

3.15

分隔符 delimiter

用于描绘数据域的开头和结尾的一组字符。

3.16

加密 encipherment encryption

为产生密文(即隐藏数据信息内容)，通过密码算法进行的(可逆的)数据变换。

3.17

十六进制数 hexadecimal digit

在0～9、A～F(大写字母)范围内代表一个4比特串的单个字符。

3.18

鉴别密钥标识符(IDA) identifier for authentication key (IDA)

标识鉴别报文时所用的密钥的域。

3.19

报文鉴别码(MAC) message authentication code (MAC)

MAC算法输出的比特串。

3.20

报文鉴别码(MAC)算法 MAC algorithm

密码校验函数

用于将比特串和秘密密钥映射到固定长度比特串的函数的算法。

注1：该算法应满足下述两个特性：

——对于任一固定密钥和任一输入比特串，函数能被有效计算；

——对于任一固定密钥，该密钥未知情况下，即使已知使用该固定密钥的函数的若干输入值和相应输出值，甚至可以自己选择输入值的情况下(已知前 i 个输入和输出，自己选择第 $i+1$ 个输入)，计算使用该固定密钥的对应于一个新的输入值(第 $i+1$ 个)的函数输出值(第 $i+1$ 个)，在计算上是不可行的。

注2：计算的可行性取决于用户的特定安全要求及环境。

3.21

报文元素 message element

为特定用途指定的一组连续字符。

3.22

报文标识符(MID) message identifier (MID)

系统跟踪审计编号(已被替代)

在给定范围(例如DMC)内，用以惟一标识金融报文或交易(例如，发送银行交易参考号)的域。

注：在ISO 8583中，MID为系统跟踪审计编号(STAN)。

3.23

报文正文 message text

在接收方和发送方之间传输的信息，不包括用于传送的头尾信息。

3.24

当前随机数 nonce

仅使用一次的序号。

3.25

接收方 receiver

接收报文的一方。

3.26

发送方 sender

对报文承担责任并被授权发送的一方。

3.27

起息日 value date

资金可由受益人进行支配的日期。

4 保护

重要信息：完整性保护仅适用于被选择的鉴别元素，报文的其他部分可能受到未被察觉的更改。用户保证所提交数据的完整性是很重要的。

4.1 鉴别密钥的保护

鉴别密钥是由发送方和接收方预先约定的用于鉴别算法中的秘密密钥。这些密钥应为确定的方式或伪随机方式产生的(见附录 F 和附录 G)。用于鉴别的任何密钥应予以保护以防止泄露给未授权方。鉴别密钥的使用应仅限于发送方和接收方(或其授权代理)之间，并且仅用于鉴别目的。密钥应按 ISO 11568 或 ISO 8732:1988 的规定进行管理。

如果 MAC 由安全密码设备计算得出，这样鉴别密钥可被很好的保护。该密钥仅在密码设备中为明文形式，且该设备应符合 ISO 13491 中的规定。

4.2 鉴别元素

MAC 计算应包括要求保护以防止欺诈性变更的那些数据元素，这些数据元素由发送方和接收方之间协议规定。MAC 计算中包含所有这些报文元素。

根据双方协议，MAC 计算中也可包括报文中未被传送的数据元素(例如：可由双方通过共享信息计算得到的填充比特或填充数据)。

选择 MAC 中包括的数据取决于其特定应用。下述元素只要出现在报文中均应纳入到 MAC 计算中：

a) 交易金额；
b) 币种；
c) 鉴别密钥标识符(IDA)；
d) 被贷记方或被借记方的标识符；
e) 受益方标识符；
f) 起息日；
g) 报文标识符；
h) 日期和时间；
i) 交易处理标识符。

4.3 重复或丢失文本的检测

应采用适当技术检测重复或丢失。在不进行进一步的报文交换的情况下，如果能惟一标识交易，则接收方仅能检测到先前交易的重放，然后接收方应检测该惟一标识信息并未出现过。此外，为检测丢失文本，应按顺序对交易进行标识。上述条件可通过在 MAC 计算中包含某些元素(即，报文元素或密钥元素)实现，这些元素对于交易是惟一的且将该交易与前一交易惟一关联。可通过下述方式的任一种实现：

a) 在 MAC 计算中包含一个特定的交易参考号，该参考号在系统的生命期中是不重复的。例如该参考号可能包括发送方 ID、接收方 ID、交易号和日期；
b) 在 MAC 计算中包含报文标识符(MID)。在下述两种情况发生之前 MID 是不被重复的：
   - 日期变更，即：计算 MAC 的日期(DMC)，或；
   - 用于鉴别的密钥加密周期的终止。

不论哪种情况先出现。即，不能出现一个以上的具有同一日期和同一报文标识符并使用相同密钥

的报文。

MID 可以由固定格式报文中的惟一的发送行交易参考号组成。附录 E 给出了保护的方法。MID 也可以包含 DMC 的日期或为一单独域。

c) 对一个交易使用惟一密钥，该密钥可以是：

- 从先前的交易密钥导出一个新的交易密钥(见 ISO 11568-2:1994 的示例和附录 G)，或；
- 使用惟一的交易参考号导出密钥，见附录 G。

d) 结合上述所有技术。

5 报文鉴别过程

5.1 准备阶段

实施者应对应用进行风险评估以确定应保护的数据(见第 4 章)、要求的密钥长度和 MAC 算法，并就下述内容达成一致：

——分组密码算法(如果 MAC 算法从 ISO/IEC 9797-1:1999 中选出)；

——哈希函数(如果 MAC 算法由 ISO/IEC 9797-2:2002 中选出)；

——填充方法(如果 MAC 算法由 ISO/IEC 9797-1:1999 中选出)；

——MAC 的比特长度；

——密钥变更频率(该内容应将加密分析技术的当前情况考虑在内)；

——通用的密钥的导出方法(如果 MAC 算法要求)。

附录 A 中给出了核准的分组密码算法。

通信双方也应交换秘密的鉴别密钥。

在全面理解潜在风险的管理和评估的基础上(见 ISO 13491)，金融服务应用宜仅在很小心的情况下使用长度小于 112 比特的密钥，通常宜使用长度不小于 112 比特的密钥。采用 112 比特 MAC 算法密钥时，推荐使用 ISO/IEC 9797-1:1999 中 MAC 算法 1 和算法 3(见第 6 章)。

发送方应使用选择的数据元计算 MAC。MAC 附加在传送的报文文本后，使其可被接收方识别。接收方应采用本章中给出的鉴别方法重新计算。如果收到的 MAC 和计算得出的 MAC 相等，则报文鉴别通过。

执行者也应考虑 6.3 中给出的性能及效率特性。

5.2 报文格式

发送方应采用接收方同意的方法格式化及编码报文。

5.3 密钥生成

基于与接收方的双方协议，报文的发送方可能会为计算 MAC 而生成新的密钥。这种密钥的导出涉及交易和与报文相关的数据。附录 F 和附录 G 给出了密钥产生和导出的部分示例。

5.4 MAC 生成

报文的发送方应使用按双方约定的顺序排列的传送报文中的鉴别元素来生成(例如，以其在报文中出现的顺序)MAC，这些鉴别元素是那些要受已核准的鉴别算法(见第 6 章)保护的传输报文元素。算法应通过一鉴别密钥激活，该密钥仅由通信双方知晓。该过程产生的 MAC 应被包含在原始报文文本中。

5.5 MAC 的放置

MAC 应放于：

a) 报文中为 MAC 指定的域，或；

b) 如果没有指定 MAC 域，附加在报文数据的尾部。

若为了传输的目的，分配域的长度超过 MAC 长度时，则 MAC 应在该域内左对齐放置。

5.6 MAC 校验

接收方一接收到报文，应使用鉴别元素、同一鉴别密钥以及同一算法计算参考 MAC。当接收方计算的参考 MAC 与在报文中接收到的 MAC 一致时，鉴别元素的内容和报文源的真实性得到确认。

接收的 MAC(及其分隔符)不应包含在算法计算中。

MAC 的计算受鉴别元素处理顺序不同的影响(即，MAC 生成后鉴别元素顺序的变化将导致鉴别的失败)。

6 核准的 MAC 算法

6.1 ISO/IEC 9797-1:1999 概述

6.1.1 算法 1 到算法 6

MAC 算法应为 ISO/IEC 9797-1:1999 中规定的一种方法。本章给出了算法特性的解释以及这些算法与 ISO 8731 和 ISO 9807 替代标准中算法间的对应关系。

ISO/IEC 9797-1:1999 中规定了采用秘密密钥和 n 比特分组密码算法计算 m 比特 MAC 的 6 种 MAC 算法。ISO/IEC 9797-1:1999 中规定的算法是基于分组密码操作模式的密码分组链接(CBC)给出的。

注 1：在 ISO/IEC 9797-1:1999 附录 B 给出的安全分析提供了防止密钥伪造和密钥恢复攻击的实施建议。

注 2：在 ISO/IEC 10116 中给出了标准的 n 比特分组密码操作模式。

——MAC 算法 1：采用单一密钥的 CBC-MAC；

——MAC 算法 2：算法 1 的变种，采用另一个密钥对算法 1 的计算结果进行一次附加的最终变换；

——MAC 算法 3：算法 1 的变种，对算法 1 的计算结果进行两次附加变换，第 1 个变换采用另一个密钥，第 2 个变换采用与算法 1 相同的密钥；

——MAC 算法 4：算法 2 的变种，在使用算法 2 计算前使用另一个密钥对数据进行一次初始变换，用算法 2 计算；

——MAC 算法 5：先用 2 个不同的单一长度密钥分别对数据进行算法 1 计算，再将 2 个计算结果做逐比特异或；

——MAC 算法 6：先用 2 个不同的密钥分别对数据进行算法 4 计算，再将 2 个计算结果做逐比特异或，其中算法 4 的计算采用双倍长度密钥。

MAC 机制的安全强度取决于密钥长度(以位表示)和保密性、分组密码的分组长度 n(以位表示)和分组密码算法强度、MAC 的长度 m(以位表示)以及特定的 MAC 算法。

6.1.2 与替代标准的关系

本条款给出了 ISO/IEC 9797-1:1999 与其他目前已被废止的标准中规定的算法间的关系，见表 1。

表 1 ISO/IEC 9797-1:1999 与替代标准的关系

标准	ISO/IEC 9797-1:1999 算法	分组密码算法	分组大小(n)	填充方法	MAC 大小(m)
IS 8731-1 [ANSI X9.9]	1	DEA(ANSI X3.92:1981)	64	1	32
IS 9807 [ANSI X9.19]	1 或 3	DEA(ANSI X3.92:1981)	64	1	32

6.1.3 最小密钥长度

MAC 应采用至少 112 比特的密钥(如果密钥长度不足 112 比特,可参考 5.1 的相关建议)。

6.1.4 推荐方法

本条给出了 ISO/IEC 9797-1:1999 推荐采用的方法,见表 2。

ISO/IEC 9797-1:1999 中给出了 6 种 MAC 算法,但针对金融服务业本标准推荐两种方法:

——采用 3-DEA 的算法 1;

——采用 DEA 的算法 3。

表 2 推荐方法

ISO/IEC 9797-1:1999 算法	分组密码算法	分组大小(n)	密钥长度	MAC 大小(m)
1	3-DEA(ANSI X9.52:1998)	64	112	$32 \leqslant m \leqslant 64$
3	DEA(ANSI X3.92:1981)	64	112	$32 \leqslant m \leqslant 64$

在 ISO/IEC 9797-1:1999 附录 B 给出的安全分析提供了防止伪造和密钥恢复攻击的实施建议。

如果采用算法 1,则应采纳 ISO 9797-1:1999 附录 B 中规定的步骤来防止 xor 伪造攻击。合适的防范措施是使用填充方法 3。

如果采用算法 3,则应限制用同一密钥产生的 MAC 数量。为保证不对 MAC 产生设备的生命周期构成限制,推荐采用会话密钥(见附录 G)。

直接伪造:如果使用填充方法 1,则对方可直接在数据串增加或删除一系列后缀'0'而不改变 MAC。这意味着填充方法 1 应仅用于数据串长度为双方预先可知的环境,或者具有不同数量后缀'0'的数据串具有相同的语义。

6.2 ISO/IEC 9797-2:2002 概述

ISO/IEC 9797-2:2002 中规定了三种使用密钥和产生 n 比特结果的哈希函数(或其轮函数)计算出 m 比特 MAC 的算法。该哈希函数选自 ISO/IEC 10118-3:1998 标准(通常称为 SHA-1、RIPEMD-160 和 RIPEMD-128)。

报文鉴别机制的安全强度取决于密钥的长度(比特数)和密钥的保密性、哈希函数的长度 n(比特数)及其算法强度、MAC 的长度 m(比特数)以及使用的指定算法。

——哈希函数 1:ISO/IEC 9797-2:2002 中规定的第 1 种算法,通常称为 MDx-MAC。该算法调用一次完整哈希函数,但对轮函数进行了小的修改,即将一个密钥增加到轮函数的附加常量中;

——哈希函数 2:ISO/IEC 9797-2:2002 中规定的第 2 种算法,通常称为 HMAC。它调用二次完整哈希函数;

——哈希函数 3:ISO/IEC 9797-2:2002 中规定的第 3 种算法,是 MDx-MAC 的变种。该算法只允许输入短字符串(最大为 256 比特)。它为只输入短字符串的应用带来了更高效率。

6.3 实施建议

在对 ISO/IEC 9797-1:1999 和 ISO/IEC 9797-2:2002 的机制进行选择时有一个简单的标准,即是否拥有该分组密码算法或哈希函数的实现。其他的标准决定严格的参数选择。例如,当使用 DEA 作为分组密码算法时会出现下述差别:

——ISO/IEC 9797-1:1999 的机制通常比 ISO/IEC 9797-2:2002 的机制慢,特别是软件方面;

——ISO/IEC 9797-1:1999 的机制比 ISO/IEC 9797-2:2002 的机制要求内存少;

——ISO/IEC 9797-2:2002 的机制能提供较长的 MAC(最大 160 比特);

——ISO/IEC 9797-2:2002 的机制 1 和 2 所用的密钥比 ISO/IEC 9797-2:2002 的机制 1 和 2 所用的短(单一 56 比特 DEA 的算法 1 不适用)。

表 3 和表 4 给出了采用 DEA 和 3-DEA 作为基本分组密码算法的 ISO/IEC 9797-1:1999 以及采用 SHA-1/RIPEMD-160 或 RIPEDMD-128 作为基础哈希函数的 ISO/IEC 9797-2:2002 的相关性能特点。

如果以 3-DEA 作为基本分组密码算法使用算法 1(代替 DEA),那么 DEA 计算量应增至 3 倍。

在 ISO/IEC 9797-1:1999 附录 B 中给出了所有 MAC 算法的安全性比较。

表 3 采用 DEA 的 ISO/IEC 9797-1:1999 相关性能

ISO/IEC 9797-1:1999 分组密码算法	分组密码算法	MAC 大小	MAC 算法密钥长度	用于评价报文大小的轮函数/分组密码数量		
				8 字节	64 字节	1 kB
1	DEA	≤64	56	1 到 2	8 到 9	128 到 129
2	3-DEA	≤64	112	2 到 3	9 到 10	129 到 130
3	DEA	≤64	112	3 到 4	10 到 11	130 到 131
4	DEA	≤64	112	4 到 5	10 到 11	130 到 131
5	DEA	≤64	56	2 到 4	16 到 18	256 到 258
6	DEA	≤64	112	8 到 10	20 到 22	260 到 262
注:后三列值的范围取决于所用的填充方法。						

表 4 ISO/IEC 9797-2:2002 相关性能

ISO/IEC 9797-2:2002 算法	哈希函数	MAC 大小	密钥长度	用于评价未填充报文大小的轮函数数量		
				8 字节	64 字节	1 kB
1	SHA-1 或 RIPEMD-160	≤160	≤128	8	9	24
1	RIPEMD-128	≤128	≤128	8	9	24
2	SHA-1 或 RIPEMD-160	≤160	160…512	4	5	20
2	RIPEMD-128	≤128	128…512	4	5	20
3	SHA-1 或 RIPEMD-160	≤80	≤128	7	*n/a*	*n/a*
3	RIPEMD-128	≤64	≤128	7	*n/a*	*n/a*
注 1:对于一固定密钥,中算法 1 和 3 的预计算可节省 6 个哈希计算。 注 2:算法 3 的报文长度限制为最大 32 个字节。						

附 录 A
（规范性附录）
核准的报文鉴别用分组密码算法

A.1 介绍

ISO/IEC 9797-1:1999 给出了 6 种基于分组密码的 MAC 算法，但对分组密码算法本身未做规定。本附录目的是直接或通过引用来指定给出 ISO/IEC 9797-1:1999 核准的分组密码算法。本标准也规定了将分组密码算法纳入该附录中的程序。

A.2 核准的分组密码算法：DEA

DEA 见 ANSI X3.92:1981。它是一个 64 比特分组密码算法，密钥的有效位为 56 比特。

A.3 核准的分组密码算法：3-DEA

3-DEA 见 ANSI X9.52:1998。它是一个 64 比特分组密码算法，密钥的有效位为 112 或 168 比特。

A.4 可选分组密码算法的审查程序

A.4.1 来源

为加入本标准而提出的可选鉴别算法应由国家标准机构提交给国家密码相关管理部门，或征得国家标准机构的同意后提交给国家密码相关管理部门。

A.4.2 提案理由

提出者应给予以下说明：

a) 希望达到的目的；
b) 该提案比本标准现有算法更好的达到该目的原因；
c) 其他地方未予描述的优点；
d) 使用新算法的经验。

A.4.3 文档

所提算法在提交审查时应具备完备的文档，包括：

a) 提出算法的完整描述；
b) 对算法满足本标准要求或与其一致的明确说明；
c) 用于计算 MAC 的处理过程的逻辑流程图；
d) 任何新术语、参数或引入变量的定义及解释；
e) 鉴别密钥的要求、用法及操作说明；
f) 以一个典型的金融报文为例，逐步描述计算 MAC 的步骤（参见附录 C）；
g) 提交前有关该算法测试情况的详细资料，特别是关系到算法安全、稳定和可靠性的信息。这些

信息应包括所使用的试验步骤的概要、试验结果以及进行试验和验证结果的机构或组织的身份(即,应提交充分的信息以使另一机构能够进行相同试验并比较得到的试验结果)。

A.4.4 公开性说明

任何提交批准的算法都不属于任何级别的保密资料。如果已对算法的版权提出申请,则应按照国家相关程序对其进行评估。所有的算法文件对于任何个人、组织或机构应为公开信息,以便进行审阅及测试。

A.4.5 提案的审查

每个新提案均应经国家相关机构审查,并在接到申请后的180天内准备一个有关报告(见A.4.6)。报告应说明是否提案资料已齐全,是否已对其进行适当试验及证明,以及提出的算法是否符合国内标准的条件及要求。也可建议提交该提案进行公开审查(见A.4.6)。

A.4.6 公开审查

当上述报告建议进行公开审查,被认为适合接纳的申请应提交给在该领域权威机构接受公开审查。这些机构和协会在接收到的90天内对提案进行审查并提交报告。

注:公开审查的周期可延至180天以准备提案的报告(见A.4.5)。

A.4.7 申诉程序

提案被拒绝时(见A.4.5),发起人可要求国内相关机构就该提案进行审核(见A.4.6),审核结果即为最终结果。

A.4.8 新鉴别算法的并入

被推荐接受的新鉴别算法连同有关的审核报告一起分发,并对是否并入本标准进行书信投票表决。

A.4.9 维护

对通过本标准描述的步骤而被采纳的算法进行定期复核,间隔不超过5年。

附 录 B
（资料性附录）
编码字符集的报文鉴别

B.1 格式选项

本附录为欲鉴别的数据编码提供了5种选项：

——二进制数据(B.3)；

——编码字符(B.4)整个报文文本，不编辑；

——编码字符(B.5)抽取的报文元，不编辑；

——编码字符(B.6)整个报文文本，编辑；

——编码字符(B.7)抽取的报文元，编辑。

选项1用于二进制字符串数据的鉴别。

选项2和选项3用于当传送介质对于字符集透明时编码字符集中数据的鉴别(例如，根据开放系统互联(OSI)模式设计的系统和网络)。

选项4和选项5用于当传送介质对于使用的字符集不透明时，受限制编码字符集中数据的鉴别(例如，博多机、电传和很多国际记录承运商提供的存储转发服务)。

格式选项的选择由通讯双方决定并符合双方协议。

如ISO/IEC 9797-1:1999附录B指出的，当使用填充方法1(或方法2)的算法1时，防止异或伪造攻击是很重要的。这可以通过接收者获知报文的长度或报文内用分隔符分开的域的数目来实现。

B.2 编码字符集(选项2～5中使用)

B.2.1 已定义的报文元素格式

B.2.1.1 通则

DMC，IDA，MAC和MID的域格式应分别符合本标准中格式的要求。其他报文元的格式未被规定。

域格式应作为鉴别过程的一部分被验证。如果使用的鉴别选项进行了编辑，则域格式应在编辑前进行验证。如果出现格式错误，则报文鉴别失败。域格式定义如下面几节所述。

B.2.1.2 DMC

发送机构发出报文的日期应按照GB/T 7408要求以世纪、年、月、日表示(最好为紧凑形式，即CCYYMMDD)，如19851101为1985年11月1日。

B.2.1.3 IDA

该域为用于鉴别的密钥的标识符且应符合ISO 8732:1988中密钥标识符的要求。

B.2.1.4 MAC

MAC应以十六进制的四组字符表示，每组四个字符中间用一个空格隔开(hhhh b hhhh b hhhh b hhhh)；例如，5A6F b 09C3 b CD86 b 1FA4。

B.2.1.5 MID

报文标识符应用1～16个可打印字符表示(AAAAAAAAAAAAAAAA)。允许字符为0～9、

A～Z(大写字母)、空格(b)、逗号(,)、句点(.)、斜线(/)、星号(*)以及连接符(-)。例如,FN-BC/2.5。

B.2.2 隐含分隔符

如果隐含分隔符在报文中位置固定或以标准化格式规则被明白无误的标识,则可以实现报文元素的隐含分隔。为实现鉴别,应对有线服务商规定的作为隐含分隔符的域名称、序号或标识域标签做处理。

B.2.3 显示分隔符

B.2.3.1 通则

显示分隔符可用于标识报文元(包括 MAC)的开始和结束。这些分隔符可用于所有编码字符集选项。显示分隔符规定如下。

B.2.3.2 DMC

示例:QD-和-DQ,例如,QD-YYMMDD-DQ。

B.2.3.3 IDA

QK-和 KQ。例如,QK-1357BANKTOBANKB-KQ。

B.2.3.4 MAC

QM-和-MQ。例如,QM-hhhhbhhhh-MQ。

B.2.3.5 MID

QX-和-XQ。例如,QX-aaaaaaaaaaa-XQ。

B.2.3.6 其他报文元

QT-和-TQ。例如,QT-文本-TQ。

在 QT-文本-TQ 中分隔的"text"可为通讯服务允许的任意长度。

B.2.4 分隔符的使用

分隔符的开始和结束应成对出现,中间不能插入显示分隔符。

注:如果此条件不满足,报文鉴别失败。

报文可能包含若干的分隔"text"域;然而,DMC、MID、IDA 和 MAC 域在每个报文中出现次数不应超过一次。

连接符应出现在所有显示分隔符中。

B.2.5 字符表示

输入算法中的鉴别元素的所有字符应以 8 比特字符表示,它包括 ISO 646 中的 7 比特代码(不包括国家字符分配值),前跟 0 开头(例如,0,b7,b6……b1)组成。当这些鉴别元素需要译码时,此译码仅用于内部计算。如果报文被转换为不同字符集,则在鉴别过程前应进行逆向转换。

B.2.6 头尾信息

为传送而增加的报文头和报文尾信息(例如,由网络增加)应被忽略(即,不应作为报文正文的一部分或被包含在算法计算中)。

B.3 选项 1:二进制数据

鉴别算法应用于整个报文正文或部分报文正文中,取决于发送方和接收方间的协议。

B.4 选项 2:编码字符;整个报文;不编辑

报文被自动处理且发送方和接收方间报文结构的准确内容均未发生变化,则算法可适用于整个报文。

MAC 对整个报文正文进行计算(见附录 C 示例)。

B.5 选项 3:编码字符;抽取的报文元;不编辑

当无法对整个报文进行鉴别时,鉴别算法应仅应用于抽取出的报文元。MAC 的计算应根据抽取出的元素并按照其出现的顺序完成(见附录 C 示例)。

鉴别的报文元应根据下述规则抽取:

a) 除了报文元和其相应分隔符删除所有字符;

b) 在每一隐含分隔报文元后插入一个空格。

B.6 选项 4:编码字符;整个报文;编辑

应对按下述规则编辑的报文文本计算 MAC(见附录 C 示例)。

在用鉴别算法处理前应按照给出顺序对所有报文元(隐含和显示分隔)进行编辑。

a) 每个回车符和换行符应用一单个空格代替;

b) 小写字母(a～z)应转换为大写字母(A～Z);

c) 除了字母 A～Z、数字 0～9、空格、逗号(,)、句点(.)、斜线(/)、星号(*)、开括号和闭括号以及连接符(-)外的所有字符均应被删除;因此,正文结束以及其他格式和控制字符应被删除;

d) 所有前导空格应被删除;

e) 每个连续空格序列(中间和结尾)应由一单个空格代替。

B.7 选项 5:编码字符;抽取的报文元;编辑

该选项与选项 3 的使用方法一致。

根据选项 3 的规则抽取报文元。

采用选项 4 的编辑规则。

B.8 "失败的"报文鉴别码(MAC)

B.8.1 无法产生 MAC

当 MAC 自动生成时,即由鉴别元素的自动抽取产生,由于违反规则,处理过程可能失败(例如,由于嵌套分隔符)。在此情况下,至少应要求人工读取(例如,纸制、屏幕或缩微胶片),则应用 8 个空格,每组四个共两组表示失败。这两组空格以一非十六进制数的字符分隔,最好为星号(*)(例如,当无法使用空格时,应用 0 代替空格,即 0000 * 0000)。

B.8.2 收到的 MAC 无法鉴别

当接收的 MAC 与鉴别过程中产生的参考 MAC 不相等时(要求 MAC 具有人工可读性),应采用在收到 MAC 空格处插入一非十六进制的可打印字符表示鉴别失败。如果字符集允许,可采用 * 表示(例如,5A6F * 09C3)。

B.9 鉴别密钥

鉴别密钥是发送方和接收方预先交换的用于鉴别算法的秘密密钥。该密钥应随机或伪随机产生(参见附录 F)。用于报文鉴别的密钥不应用于其他目的。任何用于鉴别的密钥不应泄漏给未授权方。

附 录 C
（资料性附录）
编码字符集报文鉴别的示例

C.1 MAC 示例一览

C.1.1 概述

本附录给出了采用 DEA 和 3-DEA 的编码字符集的报文鉴别示例。这些示例说明了表 C.1 所示的 ISO/IEC 9797-1:1999MAC 算法的使用方法。

注：本附录中包含的所有计算应在采用 ECB 和 XOR 选项的单个数据组进行，且结果应采用 CBC 在整个数据组的集合上验证。

表 C.1 MAC 计算示例总表

示例	报文元	ISO/IEC 9797-1:1999 算法	填充方法	分组密码算法	块大小（n）	有效密钥比特	MAC 大小（m）
1	所有	1	1	3-DEA	64	112	$32 \leqslant m \leqslant 64$
2	经选择的	1	1	3-DEA	64	112	$32 \leqslant m \leqslant 64$
3	所有	3	1	DEA	64	112	$32 \leqslant m \leqslant 64$

如 ISO/IEC 9797-1:1999 附录 B 指出的，当使用填充方法 1（或方法 2）的算法 1 时，防止异或伪造攻击是很重要的。这可以通过接收者获知报文的长度或报文内用分隔符分开的域的数目来实现。

示例采用了由 ATM 产生的交易报文，并且包括了一加密 PIN 块。

示例 1 和示例 3 采用整个报文用于 MAC 计算。仅使用报文文本（整体）而不包括协议相关域，如报头。示例 2 说明了仅采用报文选择域的 MAC 计算。

如 5.1 规定，鉴别算法采用密码分组链接（CBC）工作模式。

示例中使用的密钥和数据块的符号应符合 ISO/IEC 9797-1:1999 的要求。

C.1.2 假定预定义协议

以 ASC II 字符（每个字符 2 个十六进制数）的十六进制形式表示鉴别元素。产生 MAC 的十六进制数为传送应转换为 ASC II 字符形式—MAC 的每个十六进制数应以 ASC II 字符的 0～9、A～F 进行传送。

注：在其他条件下，预定义协议对于鉴别元素和 MAC 传送可能规定其他形式。例如，按比特存取协议，二进制数可能用于下述两种情况，减少 MAC 计算时间和 MAC 传送时间。

C.1.3 输入报文示例

下述给出输入报文文本（ASC II）的三个示例，示例中的符号¶用于表示域分隔符。

11¶918273645¶¶58143276¶¶;1234567890123456＝991210000? ¶00012500 ¶9786534124876923 ¶

表 C.2、表 C.3 给出示例报文域的简短描述。

表 C.2 输入报文样本

域名称	说 明	值
报文类型	终端表示发送报文类型的代码	11
终端 ID	终端被网络识别的号码	918273645
时间变量数	随着每次交易或报文进行变化的号码或值	58143276
第 2 磁道数据	顾客使用卡片第 2 磁道中编码的信息。该域内容在下文中详细描述	;1234567890123456=9912100007
交易数据	终端告知网络和请求的交易值和类型的域	00012500
加密 PIN Block	客户输入 PIN 被传送到加密网络所在的域	9786534124876923

表 C.3 第 2 磁道数据示例

起始符(SS)	;
主账号	1234567890123456
域分隔符	=
失效日期	9912
自由数据	10 000
结束符(ES)	?

C.2 MAC 计算示例 1

示例 1 使用整个报文文本(可被认为是单一鉴别元素)计算 MAC。对于此示例,预定义协议规定了包含分隔符和从起始符(SS)到结束符(ES)的所有卡编码数据(第 2 磁道)的内容。

加密密钥(十六进制):K=0123 4567 89AB CDEF FEDC BA98 7654 3210

第一数据块(十六进制):31311C3931383237(为 ASC II 代码 11¶91827 的十六进制形式)。所有数值以十六进制表示。

迭代 (x)	数据块 (Dx)	3-DEA 输入块 (Dx xor Hx-1)	Ⅳ/3-DEA 输出块 (Hx)
0			0000000000000000
1	31311C3931383237	31311C3931383237	827E153B886163D2
2	333634351C1C3538	B148210E947D56EA	00A37ACBAD184184
3	3134333237361C1C	319749F99A2E5D98	1AE4BE256716410E
4	3B31323334353637	21D58C1653237739	2F195D24CD861FA4
5	3839303132333435	17206D15FFB52B91	35B8FF7899281997
6	363D393931323130	0385C641A81A28A7	E156D31014362301
7	3030303F1C303030	D166E32F08061331	49FE9E6E54743E43
8	31323530301C3937	78CCAB5E64680774	4B7E8111049919F3
9	3836353334313234	7348B42230A82BC7	E355B6FF76CFFF03
10	3837363932331C00	DB6280C644FCE303	F7B47FFBD1720C55

注 1:第 1 数据块 D_1 直接输入 3-DEA。可选择的,通过将 CBC 的工作模式设置为Ⅳ可将 H_0 设为 0000000000000000。

注 2：最终数据块包括报文中的 7 个字符以及 00 的填充字节。

注 3：32 比特 MAC 为 F7B47FFB。长型 MAC 可采用附加比特从最终输出模块中抽取出来。

C.3 MAC 计算示例 2

示例 2 为仅采用下述选择报文元的 MAC 计算过程。

——时间变量序号(或值)；

——顾客卡第 2 磁道的账号(PAN)；

——交易数据；

——加密 PIN 块。

对于本示例，预定义协议规定了分隔符内容和鉴别元素的起始点。鉴别计算基于下述输入报文文本(ASC II)进行。“¶”符号用于表示域分隔符。

58143276 ¶;1234567890123456=¶ 00012500 ¶ 9786534124876923 ¶

加密密钥(Hex)K=0123 4567 89AB CDEF FEDC BA98 7654 3210

第 1 数据块(Hex)：3538313433323736(该值为 ASC II 代码 58143276 的十六进制表示形式)。所有数值以十六进制表示。

迭代 (x)	数据块 (Dx)	3-DEA 输入块 (Dx xor H_{x-1})	Ⅳ/3-DEA 输出块 (Hx)
0			0000000000000000
1	3538313433323736	3538313433323736	46813E6FA5BFB3B0
2	1C3B313233343536	5ABA0F5D968B8686	E3A6673630EF0C1E
3	3738393031323334	D49E5E0601DD3F2A	21644229B112881E
4	35363D1C30303031	14527F358122B82F	84FBC45C0F95DF19
5	323530301C393738	B6CEF46C13ACE821	3F9C8473CDF66468
6	3635333431323438	09A9B747FCC45050	1DBF9E759DF842CD
7	37363932331C0000	2A89A747AEE442CD	6B64A37C973A1548

注 1：第1 数据块 D_1 直接输入 3-DEA。可选择的，通过将 CBC 的工作模式设置为Ⅳ可将 H_0 设为 0000000000000000。

注 2：最终数据块包括报文中的 6 个字符以及 2 个 00 的填充字节。

注 3：32 比特 MAC 为 6B64A37Cf。长型 MAC 可采用附加比特从最终输出模块中抽取出来。

C.4 MAC 计算示例 3

示例 3 采用完整报文文本(可被认为是单一鉴别元素)进行 MAC 计算。对于该示例，预定义协议规定了分隔符的内容以及从起始符(SS)到结束符(ES)的所有卡编码数据(第 2 磁道)。

加密密钥(十六进制)：K=0123 4567 89AB CDEF FEDC BA98 7654 3210

K′=FEDCBA9876543210

第一数据分组(十六进制)：31311C3931383237(为 ASC II 代码 11 ¶ 91827 的十六进制形式)。所有数据以十六进制表示

迭代 (x)	数据分组 (Dx)	3-DEA 输入分组 (Dx xor Hx-1)	Ⅳ/3-DEA 输出分组 (Hx)
0			0000000000000000
1	31311C3931383237	31311C3931383237	356C20A9E60304D9
2	333634351C1C3538	065A149CFA1F31E1	BE3EDA28E5A358EA

迭代 (x)	数据分组 (Dx)	3-DEA 输入分组 (Dx xor Hx-1)	Ⅳ/3-DEA 输出分组 (Hx)
3	3134333237361C1C	8F0AE91AD29544F6	D451B35100C56A84
4	3B31323334353637	EF60816234F05CB3	BCF794DAA6BB0FFE
5	3839303132333435	84CEA4EB94883BCB	3622C2A8A5F73F94
6	363D393931323130	001FFB9194C50EA4	EA776E4F7064C650
7	3030303F1C303030	DA475E706C54F660	2ABFE53C0CA6C57D
8	31323530301C3937	1B8DD00C3CBAFC4A	0EBF212FA1E0EBB2
9	3836353334313234	3689141C95D1D986	65603056F90CA687
10	3837363932331C00	5D57066FCB3FBA87	C156F1B8CDBFB451
		C156F1B8CDBFB451	CCCD3C0841F6C7AB
		CCCD3C0841F6C7AB	C209CCB78EE1B606

注 1：第 1 数据分组 D_1 直接输入 DEA。可选择的，通过将 CBC 的工作模式设置为Ⅳ可将 H_0 设为 0000000000000000。

注 2：最终数据分组包括报文中的 7 个字符以及 1 个 00 的填充字节。

注 3：最终迭代包括附加解密 K′和加密 K。

注 4：32 比特 MAC 为 C209CCB7。可采用附加比特从最终输出分组中抽提出长型 MAC。

附 录 D
（资料性附录）
标准电传格式的报文鉴别框架

D.1 目的

本附录给出了根据本标准定义的格式鉴别电传报文所要求的附加数据的结构框架。

使用示例为 ISO 7746:1988 银行间电传报文格式中的示例 1。

发送方和接收方必须在所选的鉴别格式选项上达成一致，以保证报文被鉴别。

报文鉴别能代替测试密钥计算运用于 ISO 7746 所含的要求或提供测试密钥的任一种格式。当选择符合国际标准的报文鉴别以保护按照本标准结构化的报文的安全时，测试密钥域和相关的内容是可选的。

D.2 报文鉴别数据元

D.2.1 IDA

鉴别密钥标识符为可选数据元。如果出现该域，应放置在报文指示符 YZYZ 开始之后，该域前后应有一空行。

格式：最多 16 个字符。

D.2.2 MAC 计算日期

MAC 计算日期(DMC)等同于所有标准用户电传报文格式中的字段 DATE 中所规定的指令日期。要求提供该数据元素。格式见 GB/T 7408。

D.2.3 20 发送方参考号

报文标识符(MID)等同于所有标准用户电传报文格式中的字段 20 SENDERS REF 所规定的发送银行的交易参考号。要求提供该数据元。

格式：最多 16 个字符。

D.2.4 MAC

报文鉴别码为必选数据元。该域应放置在报文最后域的最后一行之后，前后应各跟一个空行。

格式：8 个十六进制字符(0～9、A～F)每组 4 个字符分成两组出现，中间以空格隔开(hhhh bhhhh)。

结合报文鉴别框架客户转账：标准格式(ISO 7746，例 1B)的报文示例。

45678 LONCOM G
54321 BANFIC CH
YZYZ

:IDA:6666（鉴别密钥标识符）

FROM:BANQUE FICTITIOUS,GENEVA

TO :LONDON COMMERCIAL BANK, BIRMINGHAM
DATE:19801201 (计算日期的 MAC)

::100 CUSTOMER TRANSFER

PLEASE PAY

:15 TEST KEY:1234
:20 SENDERS REF:A4760 (报文标识符)
:30 VALUE DATE:801 201
:32 AMOUNT:CHF1 .000,00
:50 ORIGINATOR:FRANZ HOLZAPFEL
:52 ORIGINATORS BANK:BANQUE DE ZUG, BAHNHOFSTRASSE,ZUG
:53 REIMBURSEMENT:WE HAVE INSTRUCTED BANQUE ANON SA,
CHIASSO TO PAY BANQUE FORTUITOUS
SA, ZUG FOR YOUR LONDON'S ACCOUNT
UNDER TELEGRAPHIC ADVICE TO YOU
:57 PAY TH. RU:NIDWAY BANK LTD, GREEN STREET,WARGRAVE
:59 BENEFICIARY:/1 22689443
H. F. JANSSEN,WALLFLOWER HOTEL WARGRAVE
:70 BENEF INFO: SALARY SEITLEMENT
:72 RECEIVER INFO:PHONE PAY THRU BANK
:82 PAY THRU INFO:PHONE BEN ON WARGRAVE 4725336

:MAC:1773 1044 (报文鉴别码)

45678 LONCOM G
54321 BANFIC CH

附 录 E
（资料性附录）
使用 MID 防重复和丢失保护

E.1 目的

通过使用每一交易特定报文元、时间变量密钥或其他方法并根据预定义协议，可实现防复制和丢失保护。本附录给出了采用 4.3 定义的 MID(报文标识符)检测传送报文的复制和丢失的方法。

也可设计出其他方法，包括本附录描述方法的变种。

E.2 防重复保护

E.2.1 重复报文

在正常状态下，如果来自一指定发送方的 MID 不重复给定的日期和给定的密钥，则重复的报文可被检测到。接收方必须检测 MID 以确保其在以前的报文中未出现过。可采用下述方法中的一种进行检测：

a) 如果 MID 未按预定顺序发送，则接收方可将接收到的 MID 与同日收到的 MID 清单进行比较；

b) 如果用特定密钥鉴别报文的 MID 总是以升序顺序发送的，则接收方只须检测标识符是否严格按照递增顺序。

还可设计出其他方法，包括上述方法的变种。MAC 序列窗口可能是必不可少的，有关窗口管理的技术见 ISO 8732:1988 的附录 D。

E.2.2 多方操作

当 2 方以上的各方共享一个公共的密钥时("多方操作")时，如果每一方都使用 MID 的一个互不相同的部分，则可检测出重复。接收方检验 MID 是否在正确的范围内，以及是否从未收到过。

E.2.3 包括身份标识

当发送方和接收方的身份标识均作为鉴别元包含在每个报文中时，接收方仅需检验它就是被期望的接收方，且该 MID 在发送方之前的报文中未出现过。在此情况下，每对发送方和接收方可使用 MID 的整个部分，且在不同双方之间的 MID 可重复。

E.3 丢失检测

如果发送方和接收方均保存有给定时间内使用的 MID 清单，则可检测出传送报文的丢失。一方给需要检测有无丢失的另一方发送该清单(通过一个具有防止重复的已鉴别的报文)。然后进行两个清单的比对。或者，如果按顺序接收 MID，则只要接收到一个乱序的 MID，接收方就可以检测出丢失的报文。当日最后一个 MID 可通过一个具有防止重复的已鉴别报文发送给丢失检测方。也可设计其他方法，包括上述给出方法的变种。

附 录 F
（资料性附录）
伪随机数发生器

F.1 介绍

本附录的目的是通过使用 n 比特分组密码算法，提供伪随机密钥 R 的产生方法。适用的分组密码算法见附录 A。

其他方法见 ISO/IEC 18031。

F.2 算法

$e[X](Y)$函数表示采用电子密码本(ECB)中的 n 比特分组密码算法，使用 X 密钥对 Y 加密。K 为仅用于产生其他密钥的密钥。V 为 n 比特种子值，该值也应保密，⊕异或操作符。DT 为日期－时间矢量，该矢量在每个密钥生成时应被更新。I 为中间值。n 比特矢量 R 的产生过程如下：

$I=e[\mathrm{K}](\mathrm{DT})$

$R=e[\mathrm{K}](I \oplus V)$

并根据下述公式生成新的 V：

$V=e[\mathrm{K}](R \oplus I)$

当鉴别算法采用 DEA 密钥时，获得的密钥的产生过程很清楚，其每一第 8 比特位为奇校验位。

对于其他算法，通过重复上述过程多遍(1，2，…，m)即可获得所要求的比特位数(小于或等于 mn)。

附 录 G
（资料性附录）
会话密钥导出

本附录描述了用于报文鉴别的会话密钥导出(SKD)原则。

会话密钥导出的目的是：

——确保每个交易或每个会话具有惟一密钥；

——防止从一个(或多个)会话密钥的信息中测定其他会话密钥(例如，通过导出装置的反转)。

会话密钥的使用能够防止要求采用同一密钥生成多个 MAC 的攻击。

一般情况下，利用发送方和接收方共享的主密钥和应用数据来导出会话密钥，该应用数据对每个交易或会话是惟一的：

Session Key = SKD(Master Key, Application Nonce)

Then

MAC = MACAlgorithm[Session Key](用于鉴别的数据)

应用 Nonce 在明文中与 MAC 进行通讯或已被接收方知晓。由于会话密钥导出是一个密钥管理活动，仅应用数据宜被包含在会话密钥导出中，该数据对于提供会话密钥的惟一性非常必要。MAC 中宜包括鉴别用应用数据。

应用 Nonce 可为发送方控制的交易计数器，并与由发送方或接收方产生的伪随机数任意组合，且被双方知晓。

MAC 算法自身可被用于 SKD 函数。如果其用于 SKD 函数，则 MAC 算法可被多次调用并需要提供足够长度的会话密钥，每次调用的输入应不同。

SKD 函数需要密集计算，通过将会话密钥从缓存的密钥(例如，之前的会话密钥)中导出，可以提高其效率。

附 录 H
（资料性附录）
一般指导信息

报文鉴别的目的是确保接收方收到的交易报文与合法指令人发出的报文完全一致。为满足此要求，报文鉴别应检测到整个伪造交易报文的欺诈插入以及其他合法交易报文的欺诈性修改。

报文鉴别不同于报文加密，因为后者不能从根本上防止修改交易，而前者不仅提供这种保护，而且对于明文报文也提供这种保护，还允许报文在处于保护状态时被解析、处理和记录。报文鉴别用于避免“主动窃取”及相关欺诈性威胁。这些是相对复杂的威胁，因为交易数据可能会通过插入通讯线路的微机系统被实时修改或插入。例如，假定某一罪犯切断了一 ATM 到其主机的通讯线路（ATM 不使用任何形式的报文鉴别），并在该线路中串联插入了一微机系统。该微机系统“看起来”像一个空闲的 ATM。对于 ATM 该系统“看起来”像主机。该欺诈性插入系统被编程以截取并抛弃每个 ATM 发出的现金请求报文，并发送一批准指令作为响应。因此，罪犯可以“提取”走 ATM 的现金，而在该过程中没有账户被借记。

报文鉴别通过对每个交易报文附加“报文鉴别码”而避免“主动窃取”欺诈情况的发生。该代码由几个校验数字组成，这些校验数字类似于奇偶校验或循环冗余校验，但这些校验数字是在加密过程中产生的。

根据发送方和接收方间的预定义协议，报文指令人产生的“报文鉴别码”或“MAC”基于整个报文或者基于报文的重要元素得到（根据预定义协议，报文中未包含的元素除了由指令人和接收方所知，应被包含在 MAC 计算中）。MAC 应包含在传送报文中，并由接收方验证，接收方持有在产生过程中使用的相同密钥。

任何试图在 MAC 产生期间和 MAC 受检测期间内修改受保护报文元的一方，其意图应被检测。由于该方不清楚密钥，因此其无法对修改后的报文产生正确的 MAC。同样的，也没有人可以成功的引入一伪造报文，因其不清楚密钥，则其无法对此报文产生适当的 MAC。

对于有效的报文鉴别，必须确保密钥的保密性。每一对通讯双方最好使用惟一的密钥，这样，密钥的泄漏将只威胁当事双方间的交易且将责任范围缩小到交易双方。

虽然报文鉴别能够检测出伪造和修改的交易报文，但其不能本质的检测出之前有效报文的欺诈性重放以及报文的缺损。附录 E 给出了这些问题的讨论。

报文鉴别不能保护报文处理中的错误和防止报文处理被干扰（报文处理在 MAC 产生前发生或者在 MAC 被验证后进行）。例如，报文鉴别不能防止不诚信商户修改其终端向客户显示交易值，该值将导致客户账户被借记（商户的账户被贷记）一个较高值。

零售 EFT 系统的参与者可有效使用报文鉴别，即使不是全部参与者均使用。不进行报文鉴别的机构可能其后会成为“主动窃取”欺诈行为的受害者，则该机构对欺诈损失负有责任，因为交易记录等将显示交易是否被欺诈性修改。鉴此，参与零售业 EFT 系统的机构能够评估执行报文鉴别的成本以及没有进行报文鉴别的成本，并据此做出决定。

参 考 文 献

[1] ISO 646 信息技术 信息交换用 ISO 7 比特编码字符集

[2] GB/T 7408—2005 数据元和交换格式 信息交换 日期和时间表示法(ISO 8601:2000, IDT)

[3] ISO 7746:1998 银行业务 银行间电传报文格式

[4] ISO 8730:1990 银行业务 报文鉴别要求(批发)

[5] ISO 8731-1:1987 银行业务 报文鉴别的核准算法 第 1 部分:DEA

[6] ISO 9807:1991 银行业务 报文鉴别要求(零售)

[7] ISO/IEC 18031 信息技术 随机数生成

[8] ANSI X9.9—1986 金融机构报文鉴别(批发)[1)]

[9] ANSI X9.17—1996 金融机构密钥管理(批发)[2)]

1) 已废止。

2) 已废止。