ICS 35.240.40
A 11

中华人民共和国国家标准

GB/T 21081—2007/ISO 13492:1998

银行业务　密钥管理相关数据元(零售)

Banking—Key management related data element(retail)

(ISO 13492:1998,IDT)

2007-09-05 发布　　2007-12-01 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

本标准等同采用国际标准 ISO 13492:1998《密钥管理相关数据元(零售)》(英文版)。

为便于使用,对于 ISO 13492 做了下列编辑性修改:

a) 规范性引用文件中所引用的国际标准,有相应国家标准的,改为引用国家标准。

b) 删除国际标准的前言。

本标准的附录 A、附录 B 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、中国农业银行、招商银行、中国银联股份有限公司、华北计算技术研究所、启明星辰有限公司。

本标准主要起草人:谭国安、杨竑、陆书春、李曙光、王林立、周亦鹏、林中、张启瑞、史永恒、赵宏鑫、李红新、徐伟、张艳、董永乐、熊少军、黄发国、李建云。

本标准为首次制定。

引　言

本标准描述了密钥管理相关数据元的结构与内容，该数据元可在银行零售业务环境下，通过电子报文方式传输，以支持密钥的安全管理。其中银行零售业务环境包括卡接收装置与收单行、收单行与发卡方之间的通信。在集成电路卡中使用的密钥以及相关数据元的密钥管理不适用于本标准。

本标准兼容银行卡报文现行 ISO 标准(见 ISO 8583)。

银行业务　密钥管理相关数据元(零售)

1　范围

本标准详细说明了密钥管理相关数据元,该数据元或者在交易报文中传输(用于保护当前交易的密钥信息),或者在加密服务报文中传输(用于保护未来交易的密钥信息)。

本标准说明了在 ISO 8583:1993 范围内应用密钥管理相关数据元的要求,应使用以下两个 ISO 8583:1993数据元:安全相关控制信息(53 位元)或密钥管理数据(96 位元)。但密钥管理相关数据的传输不局限于 ISO 8583:1993 标准。

本标准适用于对称和非对称密码系统。

ISO 11568 描述了零售银行业务环境下密钥安全管理过程。ISO 9564 和 ISO 9807 分别描述了安全性相关数据,如 PIN 和 MAC。

2　规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准,然而,鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本标准。

GB/T 15694.1—1995　识别卡　发卡方者标识　第 1 部分:编号体系(idt ISO/IEC 7812-1:1993)

ISO/IEC 7812-2:1993　身份识别卡　发卡方身份识别　第 2 部分:申请与注册程序

ISO 8583:1993　产生报文的金融交易卡　交换报文规范

ISO 8908:1993　银行业务及相关金融服务　词汇和数据元

ISO 9564-1:1991　个人识别码的管理与安全　第 1 部分:PIN 保护原则与技术

ISO 9807:1991　银行业务和相关金融服务　报文鉴别要求(零售)

ISO 11568-1:1994　银行业务　密钥管理(零售)　第 1 部分:密钥管理介绍

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

ISO 11568-3:1994　银行业务　密钥管理(零售)　第 3 部分:对称密码的密钥生命周期

ANSI X3.92:1987　数据加密算法

3　术语和定义

ISO 8908:1993 给出的以及下列术语和定义适用于本标准。

3.1

非对称密码　asymmetric cipher

加密密钥与解密密钥不同,并且由加密密钥推导出解密密钥的计算是不可行的。

3.2

密码　cipher

在称之为密钥的参数控制下,实现明文、密文之间相互转换的一组运算。

注:加密运算是将数据(明文)转换为不易理解的形式(密文)。解密运算是将密文恢复为明文。

3.3

密码算法　cryptographic algorithm

规定实现数据加密和解密过程的一套规则。

注:设计该算法使得除非通过穷举搜索否则不可能确定控制参数(如密钥)。

3.4

密码密钥　cryptographic key

密钥　key

指除非通过穷举搜索方式，否则不能从输入、输出数据推导出密码算法的控制参数。

3.5

密码服务报文　cryptographic service message

一种传递密钥或用于控制密钥关系相关信息的报文。

3.6

主密钥　primary key

用于产生交易中其他密钥的密钥(例如以变形或变换的方式)。

3.7

对称密码　symmetric cipher

使用相同的密码密钥进行加密和解密的密码方法。

3.8

交易报文　transaction message

用于传递相关金融交易信息的报文。

4　密钥管理相关数据元的要求

一个传递交易密钥相关信息的密钥管理相关数据元通常分为几个子域。该数据元可以在通信各方均隐式地掌握子域特征的交易中进行传输。在此交易环境下进行交换，各方可以使用密钥管理相关数据元作为私用域，并以各方一致同意的方式定义私用域的子域。在子域特征不是隐式的交易环境中，必须使用标准化的表示方法组织子域，以支持互操作性。然而，另外的环境中，两种类型的交易都可进行交换。

为了区分采用标准化表示方法和用于私用目的密钥管理相关数据元交易，应将密钥管理相关数据元的第一字节构造为“控制字节”，并定义如下：

00-9F：密钥管理相关数据元的第一个子域是可变长密钥集标识符，详见 4.1 和 4.2 中的定义。

A0-FF：密钥管理相关数据元是一个私用域，其中子域的特征为通信各方隐式地掌握。

密钥集标识符的使用为传递与密钥管理系统相关的密钥管理信息类型提供了标准化方法。这种方法既不需要识别特定的密钥管理技术，也不需要指定特殊子域来满足每项技术要求。

当密钥管理相关数据元以密钥集标识符开始时，数据元的其余字节包含了对交易进行密码处理的密钥所需的所有信息。因此，数据元其余字节所包含的子域没有特定的结构。任何基于每笔交易变化的信息都将随着密钥集标识符被传递。这些信息通常包括一个密钥集内的某个或某些特定密钥的标识。

在从一个交易到下一个交易过程中没有变化的密钥管理相关信息不必随着每笔交易进行传递，而是可以隐含或随着相应的密钥一同进行安装和存储。隐含信息的示例包括以下几种：

a)　用于交易密钥的密钥管理技术(例如：静态密钥、每笔交易的唯一密钥)；

b)　已加密或已鉴别的数据格式(例如：PIN BLOCK 格式)；

c)　使用的加密算法；

d)　在交易中使用不同密钥的个数以及每个密钥的目的。

在一些密钥管理方案中，可以不必在交易报文中传输密钥管理相关数据元。如果需要传输这样的数据元，相关细节详见附录 A 中的说明。

4.1　密钥集标识符的概念

密钥集标识符是一个能够唯一识别密钥集的数值，其中密钥集是那些彼此不同但是共有某些相同

特征的相关密钥的集合，最显著的特征是：

a) 所有密钥采用相同的密钥管理方法进行管理；

b) 采用同一高级别的密钥加密（用于数据库存储）或导出密钥集的所有密钥；

c) 对密钥集的所有密钥，密钥管理相关数据元的剩余字节（除密钥集标识符之外的部分）以同样的方式构建，并通过相同的逻辑进行解释。

收单行主机上的处理逻辑（如计算机软件）与任意给定的密钥集关联，可以对密钥管理相关数据元进行解释以确定在交易中使用哪些的密钥，以及如何使用每种密钥。

具有不同密钥集标识符的多个密钥集可以使用完全相同的处理逻辑，不同之处仅在于诸如密钥加密密钥或根密钥，这两种密钥分别用来为相关交易解密或导出密钥。

密钥集标识符的第一个字节是控制字节（00-9F）。密钥集标识符的分配见 4.2 节的描述。密钥集标识符的长度是可变的，且没有规定最大长度。密钥集标识符的长度是隐式的。因此，密钥管理相关数据元不应在密钥集标识符之前包含“长度”子域来表示密钥集标识符的长度。同样，密钥集标识符之后也不需要特定的分隔符（注意，如果密钥管理相关数据元在变长域内进行传输，密钥管理相关数据元之前可以是表示整个数据元长度的长度子域，见 ISO 8583:1993 中对安全相关的控制信息和密钥管理数据的要求）。

既然密钥集标识符具有可变长度，并且长度是隐式的，收单行主机可在密钥集标识符表中存储每个识别出的密钥集标识符的长度。例如，当主机从 POS 终端接收到交易时，主机在每一个这样的表条目中，宜以最左端密钥管理相关数据元位来匹配密钥集标识符，密钥管理相关数据元与特定表条目规定长度相同。这样的匹配说明表条目包含用于刚接收到的密钥管理相关数据元的密钥集标识符。

4.2 密钥集标识符的分配

为了防止机构对密钥集标识符进行重复赋值，应根据 ISO 7812 的说明使用六位发卡方识别码（IIN）或者根据 ISO 8583:1993 中的说明使用六位机构标识码（IIC）对密钥集标识符进行分配。ISO 注册机构将发卡方识别码（IIN）分配给发卡机构，将机构标识码（IIC）分配给非发卡机构。由于发卡方识别码（IIN）和机构标识码（IIC）对于机构是唯一的，且这两组编码不会重迭，这就保证了如果两个密码环境合并，在各自独立环境中唯一的密钥集标识符在合并后的环境中仍然是唯一的。

对于希望获得密钥集标识符却没有被分配 IIN 或 IIC 编码的组织也可以从分配了一个 IIN 或 IIC 的机构获得标识符。这样的机构应保证不分配重复的密钥集标识符。

如果机构不需要比分配的发卡方识别码（IIN）或机构标识码（IIC）数目更多的密钥集标识符，机构可以直接使用发卡方识别码（IIN）或机构标识码（IIC）作为密钥集标识符。如果该机构需要额外的密钥集标识符，应在发卡方识别码（IIN）或机构标识码（IIN）的右边连接一个或更多的十六进制位，并通过这种方式从一个发卡方识别码（IIN）或机构标识码（IIC）获得多个密钥集标识符。

分配密钥集标识符的机构应在分配基于 IIN 或 IIC 的任何密钥集标识符之前，选择使用多少位来与其 IIN 或 IIC 进行连接以获得密钥集标识符。例如，如果某一机构通过连接一位数字到 IIN 或者 IIC 而使用 7 位密钥集标识符，那么在已经使用所有 16 个这样的 7 位数字后，就不可再添加第八位数字以获得更多的密钥集标识符。这是因为这样的 8 位密钥集标识符的前 7 位数字与已经分配的密钥集标识符仍然匹配。例如，7 位密钥集标识符“1362047”已经存在，就不允许存在 8 位密钥集标识符“13620475”，反之亦然，因为一个密钥集标识符是完全包含在另一个密钥集标识符中的。有关密钥集标识符的应用实例详见附录 B。

5 在 ISO 8583:1993 中的实现

当第 4 章中规定的密钥管理相关数据元与 ISO 8583:1993 一起用于传递当前交易报文的密钥管理信息时，密钥管理相关数据元的内容应通过使用 ISO 8583:1993 安全相关的控制信息来进行传输，该控制信息是一个最大 48 字节的变长二进制数据元。

注 1：传输安全相关控制信息的 ISO 8583:1993 报文的一些例子如下：包含个人识别码(PIN)数据(52 比特位)的授权或金融交易请求、或者文件操作、或者包含报文鉴别代码域(64 比特位或 128 比特位)的网络管理报文。

当密钥管理相关数据元与 ISO 8583:1993 一起用于密码服务报文，传递未来使用的密钥信息时，应使用 ISO 8583:1993 密钥管理数据来传输密钥管理相关数据元的内容，ISO 8583:1993 密钥管理数据是一个最多 999 字节的变长二进制数据元。

注 2：传输密钥管理数据的 ISO 8583:1993 报文的例子如下：网络管理请求或请求响应，它们用于对当前密钥的同步进行确认或者交换未来使用的密钥。

附 录 A
（资料性附录）
传输密钥管理相关数据元的应用

A.1 传输数据的用途

在交易报文中传输密钥管理的相关信息有两个主要用途：

a） 识别用于保护当前交易报文的密钥（通常只需要验证单一主密钥）；

b） 传输用于保护日后交易报文的密钥信息。

第二个用途主要与主密钥会话密钥技术相关，传输的信息或者是主密钥加密的新会话密钥（“工作”或“交易”密钥），或是先前主密钥加密的新主密钥。

需要注意的是，在遵循 ISO 标准的零售银行业务系统中，主密钥会话密钥技术具有重大价值，当且仅当在下述条件下：

a） 主密钥比会话密钥更不容易受到穷举攻击的影响；或；

b） 在成功收到并解密新会话密钥后，主密钥自身被更换（例如：通过传输新的在原有主密钥下加密的主密钥）。

既然这样的密钥更换情况通常很少发生（例如：频率不会超过几个小时一次），传输未来密钥信息的效率就不是特别重要了。例如，（按照 ISO 8583:1993 中的说明）如果使用基本位图来传输交易数据，那么扩展位图将用于放置传输更换密钥信息的数据元。

A.2 数据描述

双方交换加密保护的交易数据时，应在不产生歧义的情况下理解以下与该交易有关每个报文的问题答案。

a） 问题 1：什么密钥将用于和交易报文有关的每个加密过程？

b） 问题 2：什么样的加密算法（例如 DEA）将用于每个加密过程？

c） 问题 3：每个加密过程是如何使用所需算法的（例如：密码块链）？

d） 问题 4：什么样的交易数据元需要得到每个加密过程的加密保护？

e） 问题 5：数据元在明文中是以怎样的格式输入到加密过程中的？

f） 问题 6：每个加密结果是以怎样的格式包括在交易报文中的？

g） 问题 7：每个加密结果存放在交易报文中的哪个位置？

h） 问题 8：密钥管理的相关信息是如何包含在交易报文中被解释的？

问题 1 通常只要求验证一个密钥——交易的主密钥。在大多数的系统中，一个交易中使用的各种密钥都是通过从单一主密钥提取变量（或变换）获得的。为了符合本标准的要求，一个通信中双方使用的主密钥通常不同于另一个通信中双方使用的主密钥，这样密钥频繁更换是正常的，甚至达到每笔交易使用一个唯一密钥的程度。

与问题 1 不同，问题 2～8 的答案在设备生命周期中通常不会改变，至少很长时间不变。既然每个加密设备通过手动的过程赋予初始密钥，问题 2～8 的答案一般在设备安装或分发初始密钥的时候予以指明。通常不会改变这样的条目，且不重复初始密钥分发过程。

通常情况下，通讯双方保留各自以加密方式存储的共享密钥（“存储密钥”方法）。因此，问题 2～8 的答案，如果在安装设备时不具体指明，可能在初始密钥分发的过程中被交换，并可能和加密密钥一起被存储。这样，通常是没有必要以交易报文方式去传递这些条目的细则。

不仅问题 2～8 的答案长时间内通常是固定的，它们对于由电子数据处理（EDP）设备连接起来的各

方通常都是相同的。然而，如上所述，主加密密钥（问题 1）对于通讯方中每两方来说通常是不同的，并随着时间改变。

A.3 显式密钥鉴定

在交易报文中传递密钥管理的相关信息首要用途——识别用于保护该报文的密钥——要求在每个这样的交易报文中存有密钥管理相关数据元。因此，效率是非常重要的，并且这样的数据元宜以基本位图的形式进行传输。此外，按照以后的论述，当数据元用作密钥标识符的时候，需要进行数据元的标准化构建。

在每一个交易报文中包含被指定类型的密钥验证信息被称为显式密钥鉴定。另一种称为隐式密钥鉴定。通过隐式密钥鉴定，从其他交易有关信息中确定用于当前讨论的交易报文的密钥。例如，即将使用的密钥可由收到信息的通信线路来确定，或者由包含在信息中、用于其他用途的“终端标识符”来确定。事实上，所有主机对主机的交易报文使用隐式密钥鉴定，许多终端对主机的交易报文也使用隐式密钥鉴定。

A.3.1 显式密钥鉴定特征

显式密钥鉴定的特征使其在 POS 环境中非常有用，这里数量众多的 POS 与单一主机相连。在这种环境下，密钥可能不与终端本身上发生联系，但是可能和物理上独立的密码键盘（PIN pad）相关，该密码键盘独立于终端安装或取代终端。

使用显式密钥鉴定可能不需要进行密钥管理，而其他情况下需要这种管理。可安装一个 POS 终端，设置密码键盘与之相连，而不需要考虑密钥管理的要求。这样一个终端中，每个交易报文包含密钥标识符，该密钥标识符用于验证报文中使用的密钥。因此没有必要先于这个终端的第一笔交易建立密钥关系。如果终端密码键盘无效并被取代，没有必要在使用新密码键盘的第一笔交易之前通知收单主机取代的消息。

显式密钥鉴定的一个额外好处在于，可以防止密码同步的丢失。当这样的丢失发生时，是因为主叫方使用了不同于接收方预期的密钥。交易报文中的显式密钥鉴定可以消除发生任何这样的误解。

显式密钥鉴定的另一个好处在于，允许使用“导出密钥”作为常规存储密钥技术的可选择办法。通过存储密钥技术，收单主机存储与之相连的每一个终端的（已加密）密钥（以 POS 环境为例）。通过导出密钥技术，上述的密钥存储就不再需要了。主机保留相对较少数目的根密钥，每一个根密钥由许多 POS 共用。当主机从这样的终端收到一笔交易时，能够通过密钥标识符的加密过程导出在该终端使用的密钥，密钥标识符包含在使用正确根密钥的交易中。举一个简单的例子，密钥标识符可通过根密钥进行加密，由此产生的密文就是终端密钥。需要注意的是所有这样的终端相关密钥都是唯一的（假定所有的密钥都有唯一的密钥标识符），即使知道某一个终端密钥也不会获得有关其他终端的任何可用信息。

有了这项技术，主机将不必维护用于存储加密终端相关密钥的数据库，因为使用交易中的密钥标识符或者共用的根密钥，任何这样的密钥都可以通过导出方式产生。消除这样的数据库可以简化密钥管理的运营与操作过程。

需要注意的是密钥标识符是公开的，不会给攻击者提供用于确定任何相关密钥的信息。

A.3.2 密钥集

当在 POS 终端使用显式密钥鉴定时，使用密钥集的概念是非常方便的。许多（例如：数以千计）终端可以使用单一密钥集中的密钥。尽管一个密钥集中的所有密钥都是不同的（除非偶然），但所有这些密钥有以下共性：

a) 如果密钥集的主密钥在主机数据库中以加密形式存储，同一密钥加密密钥用于对密钥集中所有这些主密钥解密。如果密钥集中的主密钥是导出的，主机将使用相同的根密钥以密码方式计算所有的这些主密钥；

b) 密钥集中主密钥的管理方法相同；

c) 任何额外的密钥都通过完全相同的方式从相关主密钥中获得(例如通过使用相同的变形);

d) 验证密钥集密钥的密钥管理相关数据元以同样的方式构建,并通过相同的逻辑进行解释;

e) 存有密钥集中密钥的所有设备相同的实现 A.2 中列出的问题 2～8 的答案。或者,密钥管理相关数据元规定任一条目的实现,不同设备对任一条目的实现可能是不同的。

对于每个密钥集,主机有必要存储高级别密钥,用于解密或导出每个主密钥。也要存储涉及如何使用密钥实现所要求密码功能的信息(该信息可以是计算机程序的形式、参数序列的形式或者两种方式结合的形式)。当使用密钥存储技术时,每个密钥集也需要一个密钥列表。当使用密钥衍生技术时,不必存储每个终端信息来确定终端相关密钥(然而,应存储一些用于审计和控制用途的终端信息,但这样的终端信息偶然丢失并不影响主机确定终端密钥的能力)。因此,密钥集的概念可用于最小化和系统化主机需要存储的密钥管理信息,继而简化主机实现密钥管理的操作。

A.3.3 密钥标识符

当密钥集与显式密钥鉴定共同使用时,鉴定密钥同时鉴定此密钥所属的密钥集是很有益处的。按照 4.1 和 4.2 中的描述,这就称为密钥集标识符。在使用的时候,密钥集标识符构成密钥标识符最重要的(最左边的)部分。

当使用密钥集标识符时,密钥标识符可以包含两到三个域,如下所述:

a) 密钥集标识符;

b) 设备标识符;

c) 密钥更换计数器(可选择)。

设备标识符表示特定设备,其密钥在标明的密钥集范围之内。对已存储的密钥系统来说,设备标识符可用来为指定的密钥集在主机密钥表中定位,发现与该设备相关的密钥的位置。对导出密钥系统来说,设备标识符利用该密钥集的根密钥来密码计算原先输入该设备的密钥。

在自动进行密钥更换的系统中,密钥更换计数器可能包含在密钥标识符中。密钥更换计数器记录自初始密钥输入以来一共发生了多少次密钥更换。当每一笔交易发生一次密钥更换时,该域就成为交易计数器。当导出密钥技术中发生自动密钥更换时,需要使用密钥更换计数器(或者交易计数器)。如果存储密钥技术中发生自动密钥更换,使用密钥更换计数器(或交易计数器)也是有帮助的(能够检测密码不同步并恢复同步)。

无需采用标准化方法表示设备标识符和密钥更换计数器。所有密钥集中这些域的表示都是固定的(如前文密钥集的定义所述)。因此,与所有密钥集发生联系的是计算机软件和/或定义安全相关子域的参数。

应指出,依照本标准分配的密钥集标识符提供了一种标准化方法,该方法中显式密钥鉴定可以和非标准化安全技术和密钥管理技术共同使用。

显式密钥鉴定在 POS 环境中使用时,通常只在终端发起的交易报文中使用。一旦收单主机接收到终端发起的交易报文,主机确定(根据报文的密钥标识符)与该终端相关的当前主密钥,然后利用该密钥或者另一相关密钥来对传回终端的数据进行密码保护。由于终端已经知道该密钥,所以没有必要再发送一个密钥标识符回终端。

附 录 B
（资料性附录）
密钥集标识符应用实例

以下是收单机构如何从多个密钥集标识符中确定适用于具体交易的密钥集标识符的一个实例。在该实例中，假定收单机构认可下述五个密钥集标识符：

密钥集标识符	长度
127165	6
12716632	8
1271664	7
1271771	7
127178	6

当收单机构收到一项交易，该交易的密钥管理相关数据元起始数据为“12716648159300……”时，收单机构必须确定以上列示的五个密钥集标识符中哪一个适用于该交易。确定过程需要进行以下步骤：

步骤 1：检查第一个密钥集标识符。密钥管理的相关数据的前 6 位数字是否为 127165？如果不是，进入步骤 2。

步骤 2：检查第二个密钥集标识符。密钥管理的相关数据的前 8 位数字是否为 12716632？如果不是，进入步骤 3。

步骤 3：检查第三个密钥集标识符。密钥管理的相关数据的前 7 位数字是否为 1271664？是。

根据这个检验过程结果，收单机构确定第三个密钥集标识符适用于该项交易。而其他两个密钥集标识符不再需要评估其适用性。

中 华 人 民 共 和 国
国 家 标 准
银行业务 密钥管理相关数据元(零售)
GB/T 21081—2007/ISO 13492:1998
*
中 国 标 准 出 版 社 出 版 发 行
北京西城区复兴门外三里河北街 16 号
邮政编码:100045
http://www.spc.net.cn
http://www.gb168.cn
电话:(010)51299090、68522006
2007 年 12 月第一版
*
书号:155066·1-30271

GB/T 21081-2007