



中华人民共和国国家标准

GB/T 19584—2004

银行卡磁条信息格式和使用规范

Magnetic stripe data content and specification for bank card

2004-09-13 发布

2005-01-01 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

前 言

本标准以 GB/T 17552《识别卡 金融交易卡》为基础,参照 GB/T 14504《银行卡》、GB/T 15694.1《识别卡 发卡者标识 第1部分:编号体系》、GB/T 15120.2《识别卡 记录技术 第2部分:磁条》等相关标准编制。本标准引用并符合 GB/T 17552 的规定,对磁条卡第1磁道、第2磁道和第3磁道的数据内容进行了详细定义并对我国银行卡各磁道的使用做出了规定。

本标准自发布之日起行业标准 JR/T 0009—2000《银行卡磁条信息格式和使用规范》废止。本标准与 JR/T 0009—2000 内容上的主要区别是:银行卡的定义、卡片验证码(CVN)的使用、CVN 的算法、PIN 验证码(PVN)的使用、服务代码的取值、第1磁道的格式代码定义和取值等。

本标准由全国金融标准化技术委员会提出。

本标准由全国金融标准化技术委员会、全国信息技术标准化技术委员会归口。

本标准由中国工商银行负责组织制定。

本标准起草单位:中国工商银行、中国人民银行、中国银联股份有限公司、中国农业银行、中国银行、中国建设银行、中国标准研究中心、中国电子技术标准化研究所。

本标准主要起草人:林晓轩、单怀光、仲安妮、张艳、张宏、桂孝生、赵宏鑫、陆书春、徐敏、王云生、司马甫、杜宁、黄发国、郝建明、刘锋、王钢、王小丽、马云、魏宏、金倩、梁波。

银行卡磁条信息格式和使用规范

1 范围

本标准规定了银行卡磁条的信息格式和使用规范。

本标准适用于中华人民共和国境内发行和使用的各种银行磁条卡。

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 2659 世界各国和地区名称代码

GB/T 12406 表示货币和资金的代码

GB/T 14504 银行卡

GB/T 15120.2 识别卡 记录技术 第2部分:磁条

GB/T 17552 识别卡 金融交易卡

3 术语和定义

下列术语和定义适用于本标准。

3.1

银行卡 bank card

商业银行等金融机构及邮政储汇机构发行的具有存取现金、消费、转账结算、信用贷款等部分或者全部功能的电子支付卡片。

3.2

主账号 primary account number(PAN)

标识发卡机构和持卡人信息的号码。它由发卡机构标识、持卡人标识和校验数组成。它是进行金融交易的主要账号。

3.3

发卡机构标识 issuer identification

标识发卡机构的代码。

3.4

持卡人标识 individual account identification

标识持卡者的代码。

3.5

校验数 check digit

位于持卡人标识之后的一位数字。它根据发卡机构标识和持卡人标识全部字符算出,用以检验输入数据的正确性。

3.6

第一辅助账号 first subsidiary account number(SAN-1)

除主账号之外的第一个可供选用的辅助账户标识。

3.7

第二辅助账号 second subsidiary account number(SAN-2)

除主账号和第一辅助账号之外的第二个可供选用的辅助账户标识。

3.8

个人标识代码 personal identification number(PIN)
持卡者的个人密码。

3.9

卡片验证码 card verification number(CVN)
对磁条信息合法性进行验证的代码。

3.10

PIN 验证码 PIN verification number(PVN)
对个人标识代码进行验证的代码。

4 磁条

银行卡磁条的特性、编码技术及编码字符集应符合 GB/T 15120.2 中的有关要求。

5 磁道的数据内容

5.1 第 1 磁道的数据内容

第 1 磁道数据编码最大记录长度为 79 个字符,数据字段的顺序和长度应与表 1 给出的第 1 磁道数据格式一致。
第 1 磁道为只读磁道。

表 1 第 1 磁道数据格式

字 段		D=动态 S=静态	字 段 长 度	备 注
序 号	名 称			
1	起始标志	S	1	“%”,见 6.1
2	格式代码	S	1	“B”,见 6.2
3	主账号	S	13~19	见 6.3
4	字段分隔符	S	1	“^”,见 6.4
5	姓名	S	2~26	见 6.5
6	字段分隔符	S	1	“^”,见 6.4
7	失效日期	S	4	YYMM,见 6.6
8	服务代码	S	3	见 6.7
9	附加数据	S	可变	见 6.8
10	结束标志	S	1	“?”,见 6.9
11	纵向冗余校验码	S	1	GB/T 15120.2

5.2 第 2 磁道的数据内容

第 2 磁道数据编码最大记录长度为 40 个字符,数据字段的顺序和长度应与表 2 给出的第 2 磁道数据格式一致。
第 2 磁道为只读磁道。
动态字段在交易过程中可由交换者根据情况修改字段内容,静态字段只能由发卡机构修改字段内容。

表 2 第 2 磁道数据格式

字 段		D=动态 S=静态	字 段 长 度	备 注
序 号	名 称			
1	起始标志	S	1	“;”,见 6.1
2	主账号	S	13~19	见 6.3
3	字段分隔符	S	1	“=”,见 6.4
4	失效日期	S	4	YYMM,见 6.6
5	服务代码	S	3	见 6.7
6	附加数据	S	可变	见 6.8
7	结束标志	S	1	“?”,见 6.9
8	纵向冗余校验码	S	1	GB/T 15120.2

5.3 第 3 磁道的数据内容

第 3 磁道的数据内容见附录 B。

6 字段说明

6.1 起始标志(STX)

用途:标明数据的开始。

格式:1 个字符。

内容:第 1 磁道为“%”,第 2 磁道和第 3 磁道为“;”。

6.2 格式代码(FC)

用途:标明该磁道的数据格式类型。

格式:第 1 磁道为 1 个字符,第 3 磁道为 2 位数字。

内容:第 1 磁道为“B”,第 3 磁道为“99”。

6.3 主账号(PAN)

用途:标明可以处理交易的发卡机构和持卡人。

格式:13 至 19 位数字。

内容:校验数算法见 GB/T 14504。

6.4 字段分隔符(FS)

用途:标明前一字段的结束。

格式:1 个字符。

内容:第 1 磁道为“^”,第 2 磁道和第 3 磁道为“=”。

6.5 姓名(NM)

用途:标明持卡者的姓氏、名字、称谓等。

格式:2 至 26 个字符。

内容:由姓氏、姓氏分隔符、名字或首写字母、分隔符(如需要时)、中间名或首写字母、结尾圆点(当其后为称谓时)、称谓组成。最小编码数据应为一个字母字符(如姓氏)加上姓氏分隔符。

6.6 失效日期(ED)

用途:表示卡失效的日期。

格式:YYMM 形式的 4 位数字,其中:

YY——卡失效年度的后 2 个字符。

MM——年度内月份的顺序号。规定在该月份的最后一天后,卡失效。

当 YYMM 为 0000 时,表示此卡无失效日期。

6.7 服务代码(SC)

用途:标明银行卡可使用的服务类型。

格式:3 位数字。

内容:

第 1 位:

1——国际使用。

2——国际使用:指明卡片有集成电路芯片,如集成电路芯片可以使用,金融交易应由集成电路处理。

5——国内使用。

6——国内使用:指明卡片有集成电路芯片,如集成电路芯片可以使用,金融交易应由集成电路处理。

7——专用:不用于交换。

9——测试。

第 2 位:

0——普通授权。

2——必须获得发卡行或发卡行代理的联机授权。

4——除非另有双方协议明确规定,必须获得发卡行或发卡行代理的联机授权。

第 3 位:

0——服务领域无限制,要求输入 PIN。

1——服务领域无限制。

2——仅用于商品和服务。

3——仅用于 ATM,要求输入 PIN。

4——仅现金。

5——仅用于商品和服务,要求输入 PIN。

6——服务领域无限制,当有密码键盘时,提示输入 PIN。

7——仅用于商品和服务。当有密码键盘时,提示输入 PIN。

6.8 附加数据

用途:存放卡片验证码(CVN)及对发卡机构有意义的任意数据。

格式:可变,但应保证该磁道字符总数不得超过最大编码长度。

内容:卡片验证码(CVN,算法见附录 A),位置及其他内容由发卡机构自行规定。

6.9 结束标志(ETX)

用途:标明磁道上有意义数据的结束。

格式:1 个字符。

内容:“?”。

6.10 纵向冗余校验码(LRC)

用途/内容:见 GB/T 15120.2。

格式:1 个字符。

7 使用规范

所有银行磁条卡必须使用第 2 磁道。第 1、3 磁道是否使用由各发卡机构自行规定。PIN 验证码(PVN)是否使用及存放位置由各发卡机构自行规定。

金融终端进行处理时,必须同时读入并上送第 2、3 磁道信息。第 2 磁道作为交换磁道,各发卡机构在进行识别和信息交换时以第 2 磁道为准。

附录 A
(资料性附录)
卡片验证码(CVN)的算法

计算步骤如下:

计算 CVN 时使用二个 64 位的验证密钥,KeyA 和 KeyB。

1) 计算 CVN 的数据源包括:

主账号(PAN)、卡失效日期和服务代码,从左至右顺序编排。

例如 19 位 PAN、4 位卡失效日期和 3 位服务代码组成 26 个字符 CVN 数据源。

2) 将上述数据源扩展成 128 位二进制数据(不足 128 位右补二进制 0)。

3) 将 128 位二进制数据分成两个 64 位的数据块。最左边的 64 位为 Block1,最右边的 64 位为 Block2。

4) 使用 KeyA 对 Block1 进行加密。

5) 将 Block1 的加密结果与 Block2 进行异或。使用 KeyA 对异或结果进行加密。

6) 使用 KeyB 对加密结果进行解密。

7) 使用 KeyA 对解密结果进行加密。

8) 从左至右将加密结果中的数字(0~9)抽出,组成一组数字。

9) 从左至右将加密结果中的字符(A~F)抽出,减 10 后将余数组成一组数字,排列在步骤 8)的数字之后。

10) 步骤 9)的左边第一组三位数即为 CVN 值。

例:

主账号:4123 4567 8901 2345 KeyA:0123 4567 89AB CDEF
有效期:8701 KeyB:FEDC BA98 7654 3210
服务代码:111

第一步:数据源为 4123456789012345 8701 111

第二步:扩展为 4123 4567 8901 2345 8701 1110 0000 0000

第三步:Block1=4123 4567 8901 2345
Block2=8701 1110 0000 0000

第四步: 用 KeyA 对 Block1 加密 结果为:B76A DDCE 71CC C6BE

第五步: 将结果与 Block2 异或, 结果为:306B CCDE 71CC C6BE
再用 KeyA 加密, 结果为:BAE6 746F 6DE1 F0E6

第六步: 用 KeyB 解密, 结果为:B262 ABCB 9DE9 9A63

第七步: 用 KeyA 加密, 结果为:8D56 25FA 7801 1A0C

第八步: 抽出结果中的数字, 结果为:8562 5780 110

第九步: 抽出结果中的字符, 结果为:DFAA C
减 10 后, 结果为:3500 2

连接到第八步的结果之后为: 8562 5780 1103 5002

第十步 最左边三位数就是 CVN=856。

附 录 B
(资料性附录)
第 3 磁道的数据内容

第 3 磁道数据编码最大记录长度为 107 个字符,数据字段的顺序和长度应与表 B.1 给出的第 3 磁道数据格式一致。
第 3 磁道为读写磁道。

B.1 第 3 磁道数据格式

第 3 磁道数据格式见表 B.1。

表 B.1 第 3 磁道数据格式

字 段		D=动态 S=静态	字 段 长 度	备 注
序 号	名 称			
1	起始标志	S	1	“;”,见正文 6.1
2	格式代码	S	2	“99”,见正文 6.2
3	主账号	S	13~19	见正文 6.3
4	字段分隔符	S	1	“=”,见正文 6.4
5	国家代码	S	3	“156”,见 B.2.1,可选
6	货币代码	S	3	见 B.2.2
7	金额指数	S	1	见 B.2.3
8	周期授权量	S	4	发卡机构自行规定,见 B.2.4
9	本周期余额	D	4	见 B.2.5
10	周期开始日期	D	4	YDDD,见 B.2.6
11	周期长度	S	2	见 B.2.7
12	密码重输次数	D	1	见 B.2.8
13	个人授权控制参数	D	6	发卡机构自行规定,见 B.2.9
14	交换控制符	S	1	见 B.2.10
15	PAN 的 TA 和 SR	S	2	见 B.2.11
16	SAN-1 的 TA 和 SR	S	2	见 B.2.12
17	SAN-2 的 TA 和 SR	S	2	见 B.2.13
18	失效日期	S	4	YYMM,见正文 6.6
19	卡序列号	S	1	见 B.2.14
20	卡保密号	D	1	见 B.2.15
21	SAN-1	S	最大 12	见 B.2.16
22	字段分隔符	S	1	“=”,见正文 6.4
23	SAN-2	S	最大 12	见 B.2.17
24	字段分隔符	S	1	“=”,见正文 6.4
25	传递标志	S	1	见 B.2.18
26	加密校验数	S	6	发卡机构自行规定,见 B.2.19
27	附加数据	D	可变	见正文 6.8
28	结束标志	S	1	“?”,见正文 6.10
29	纵向冗余校验码	D	1	GB/T 15120.2

B.2 字段说明

B.2.1 国家代码

用途:标明可以处理由银行卡产生交易的国家。

格式:3 位数字。

内容:“156”(见 GB/T 2659);

B.2.2 货币代码

用途:标明结算时使用的货币类型。

格式:3 位数字。

内容:见 GB/T 12406。

B.2.3 金额指数

用途:决定周期授权量(B.2.4)与本周期余额(B.2.5)两字段的基值。

格式:1 位数字。

内容:表示周期授权量(B.2.4)与本周期余额(B.2.5)两字段必须乘以 10 的一个幂指数的值,以此表示货币金额。

B.2.4 周期授权量

用途:表示在一个周期内累积交易不能超过的金额。

格式:4 位数字。

内容:由发卡机构自行规定授权量。

B.2.5 本周期余额

用途:表示当前周期内的可用金额。

格式:4 位数字。

内容:在新的周期开始时,该字段等于周期授权量(B.2.4),消费后逐次递减,余额存本字段。

B.2.6 周期开始日期

用途:表示一个新周期开始的日期。

格式:YDDD 形式的 4 位数字,其中:

Y——年度最后一个有效字符。

DDD——年度内天数的顺序号,其范围为 001~366。

B.2.7 周期长度

用途:表示所有交易的累积值不能超过授权量的时间期限。

格式:2 位数字。

内容:00——本周期余额只能减少,但不能重置的一种银行卡;

01~79——本周期的天数;

80——周期为 7 天;

81——周期为 14 天;

82——周期为半个月;

83——周期为一个月;

84——周期为三个月;

85——周期为六个月;

86——周期为一年;

87~99——保留,待分配。

B.2.8 密码重输次数

用途:记录允许未成功输入密码的次数。

格式:1 位数字。

内容:该字段在发卡和正确输入密码时被赋初值,初值由各发卡机构自定义;当输入密码不正确时该字段减 1。

B.2.9 个人授权控制参数

用途:提供一种可选择的安全性能。

格式:6 位数字。

内容:保密算法由各发卡机构自行规定。

B.2.10 交换控制符

用途:标明银行卡适用于交换的范围。

格式:1 位数字。

内容:0——无限制;

1——国际使用;

2——限制在国内、跨系统交换;

3——限制在省内、跨系统交换;

4——限制在市内、跨系统交换;

5——限制在国内系统内交换;

6——限制在省内系统内交换;

7——限制在市内系统内交换;

8——管理卡,不适用于交换;

9——系统测试卡。

B.2.11 主账号(PAN)的账户类型(TA)和服务约束(SR)

用途:定义主账号(PAN)的账户类型和可提供的服务。

格式:2 位数字。

内容:a)第 1 位数字——账户类型

0——主账号(PAN)未在第 3 磁道上编码;

1——储蓄或结算账户;

2——现金或支票账户;

3——信用卡账户;

4——适用于多种账户类型的通用账户;

5——付息现金或支票账户;

6~8——保留待分配;

9——发卡机构内部使用,但不能交换。

b)第 2 位数字——服务约束

0——无约束;

1——无现金服务;

2——无销售点(POS)服务;

3——无现金和销售点(POS)服务;

4——要求肯定的授权;

5~7——保留待分配;

8~9——发卡机构内部使用。

B.2.12 第一辅助账号(SAN-1)的账户类型(TA)和服务约束(SR)

用途:同 B.2.11 中的定义一致,但此字段内容涉及第一辅助账号(SAN-1)(B.2.16)中包含的账号。

格式:2 位数字。

内容:同 B. 2. 11。

B. 2. 13 第二辅助账号(SAN-2)的账户类型(TA)和服务约束(SR)

用途:同 B. 2. 11 中的定义一致,但此字段内容涉及第二辅助账号(SAN-2)(B. 2. 17)中包含的账号。

格式:2 位数字。

内容:同 B. 2. 12。

B. 2. 14 卡序列号

用途:区别具有相同主账号(PAN)的卡(同时或连续发行)。

格式:1 位数字。

内容:由发卡机构定义,在最初发卡或卡失效后换卡时赋值。每次增加卡或发新卡时,该字段值加 1。

B. 2. 15 卡保密号

用途:用于建立磁条所含数据与物理卡的联系。

格式:字段分隔符(FS)。

内容:FS——表示卡保密号字段不在第 3 磁道上编码。

B. 2. 16 第一辅助账号(SAN-1)

用途:标明第一个可选用的辅助账号。

格式:最大 12 个字符。

内容:由发卡机构酌情使用。长度为 0 时,表示不使用第一辅助账号。

B. 2. 17 第二辅助账号(SAN-2)

用途:标明第二个可选用的辅助账户。

格式:最大 12 个字符。

内容:由发卡机构酌情使用。长度为 0 个字符时,表示不使用第二辅助账号。

B. 2. 18 传递标志

用途:提供可减少传送交换信息长度的功能。它表明交换信息是否包含附加数据的内容。

格式:1 个字符。

内容:0——包括所有附加数据;

1——不包括附加数据;

2~9——无效。

B. 2. 19 加密校验数(CCD)

用途:通过使用加密公式提供一种校验该磁道上数据完整性的方法。

格式:6 个字符。

内容:加密方法由各发卡机构自行规定。
