



中华人民共和国国家标准

GB/T 19584—2010
代替GB/T 19584—2004

银行卡磁条信息格式和使用规范

Specification on magnetic stripe data content and application for bank card

2011-01-14发布

2011-05-01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 磁条	2
5 磁道的数据内容	2
5.1 第1磁道的数据内容	2
5.2 第2磁道的数据内容	3
5.3 第3磁道的数据内容	3
6 字段说明	3
6.1 起始标志(STX)	3
6.2 格式代码(FC)	3
6.3 主账号(PAN)	3
6.4 字段分隔符(FS)	3
6.5 姓名(NM)	3
6.6 失效日期(ED)	3
6.7 服务代码(SC)	4
6.8 附加数据	5
6.9 结束标志(ETX)	5
6.10 纵向冗余校验码(LRC)	5
7 使用规范	5
附录 A (资料性附录) 第3磁道的数据内容	6
附录 B (资料性附录) 卡片验证码(CVN)的算法	10
附录 C (资料性附录) PIN 验证码(PVN)的算法	11
参考文献	12

前 言

本标准是对 GB/T 19584—2004《银行卡磁条信息格式和使用规范》的修订。

本标准与GB/T19584—2004 相比，主要变化如下：

- a) 重新起草前言并增加引言；
- b) 根据技术及业务的发展对3.1、3.5、3.8、6.3的内容进行了重新定义
- c) 将6.6中的“当YYMM 为0000时，表示此卡无失效日期”修改为“当卡无失效日期时，YYMM 写入4912”；
- d) 将表述不一致的文字进行了修改；
- e) 替换附录B 中的算法示例为银联标准卡；
- f) 增加附录C 并重新编排附录顺序；
- g) 增加参考文献。

本标准代替GB/T 19584—2004《银行卡磁条信息格式和使用规范》。

本标准的附录 A 至附录C 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：中国人民银行、中国金融电子化公司。

本标准参与起草单位：中国工商银行、中国农业银行、中国建设银行、华夏银行、中国银联股份有限公司、银行卡检测中心、中钞信用卡产业发展有限公司。

本标准主要起草人：姜云兵、杜宁、李曙光、赵志兰、刘启滨、马小琼、张艳、刘运、赵宏鑫、袁红斌、袁国能、曹瀛、黄发国、刘志刚、王飞。

本标准所代替标准的历次版本发布情况为：

——GB/T 19584--2004。

引 言

本标准以GB/T 17552《识别卡 金融交易卡》为基础，参照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《识别卡金融交易卡》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描述并对我国银行卡各磁道的使用做出了规定。

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 2659—2000,eqv ISO 3166-1:1997)

GB/T 12406 表示货币和资金的代码(GB/T 12406—2008,ISO 4217:2001,IDT)

GB/T 15120.2 识别卡记录技术第2部分：磁条(GB/T 15120.2—1994,idt ISO 7811-2:1985)

JR/T 0008 银行卡发卡行标识代码及卡号

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

由商业银行等金融机构向社会发行的，具有消费信用、转账结算、存取现金等全部或部分功能的支付工具。

3.2

主账号 primary account number

PAN

用于标识发卡机构及卡片的号码，由发卡机构标识代码、发卡机构自定义位和校验位组成。主账号等同于JR/T 0008中的卡号。

3.3

发卡机构标识代码 issuer identification number

标识发卡机构的代码。

3.4

校验位 check digit

位于主账号的最后一位数字。该数字根据校验位前的全部数字计算得出，用以检验主账号的正确性。

3.5

第1辅助账号 first subsidiary account number

SAN-1

除主账号之外的第1个可供选用的辅助账户标识。

3.6

第2辅助账号 second subsidiary account number

SAN-2

除主账号和第1辅助账号之外的第2个可供选用的辅助账户标识。

3.7

个人识别码 personal identification number

PIN

持卡人持有的用于身份验证的代码或口令。

3.8

卡片验证码 card verification number

CVN

对磁条信息合法性进行验证的代码。

3.9

PIN 验证码 PIN verification number

PVN

对个人识别码进行验证的代码。

4 磁条

银行卡磁条的特性、编码技术及编码字符集参见GB/T 15120.2。

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。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¹⁾。

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	“A”，见6.4
5	姓名	S	2~26	见6.5
6	字段分隔符	S	1	“A”，见6.4
7	失效日期	S	4	YY MM, 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	见GB/T 15120.2

1)第2、3磁道对动态字段与静态字段的写入要求与第1磁道相同。

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。

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	YY MM, 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	见GB/T 15120.2

5.3 第3磁道的数据内容

第3磁道的数据内容参见附录A。

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：标明持卡者及可以处理交易的发卡机构。

格式：13位~19位数字。

内容：等同于JR/T 0008标准的卡号。

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“A”，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个~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。

GB/T 19584—2010

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。

当卡无失效日期时, YYMM 写入4912²。

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:

0——保留待分配;

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;

3——保留待分配;

4——保留待分配;

5——国内使用;

____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;

8——保留待分配;

9——测试。

第2位:

0——普通授权;

1——保留待分配;

2——必须获得发卡行或发卡行代理的联机授权;

3——保留待分配;

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;

5——保留待分配;

6——保留待分配;

7——保留待分配;

8——保留待分配;

9——保留待分配。

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;

____仅用于商品和服务, 要求输入 PIN;

6____服务领域无限制, 当有PIN输入设备时, 提示输入 PIN;

____仅用于商品和服务, 当有PIN输入设备时, 提示输入PIN;

2) 为与当前国际通行惯例保持一致, 减少国内银行卡在境外受理时的障碍, 当卡无失效日期时, YYMM 定义为4912。

8____保留待分配;

g____保留待分配。

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, 算法参见附录B), 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: 参见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。

金融终端进行处理时, 应同时读入并完整上送第2、3磁道信息(如果第3磁道信息存在), 各交易参与方在识别、信息交换及交易处理时应以第2磁道为准。

PIN 验证码(PVN) 是否使用及存放位置由各发卡机构自行规定, 具体算法参见附录C。

附录 A
(资料性附录)
第3磁道的数据内容

A.1 第3磁道数据格式

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 A.1 给出的第3磁道数据格式一致。

第3磁道为读写磁道。

表A.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6.1
2	格式代码	S	2	“99”，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	国家代码	S	3	“156”，见A.2.1, 可选
6	货币代码	S	3	见A.2.2
7	金额指数	S	1	见A.2.3
8	周期授权量	S	4	发卡机构自行规定，见A.2.4
9	本周期余额	D	4	见A.2.5
10	周期开始日期	D	4	YDDD，见A.2.6
11	周期长度	S	2	见A.2.7
12	密码重输次数	D	1	见A.2.8
13	个人授权控制参数	D	6	发卡机构自行规定，见A.2.9
14	交换控制符	S	1	见A.2.10
15	PAN的TA和SR	S	2	见A.2.11
16	SAN-1的TA和SR	S	2	见A.2.12
17	SAN-2的TA和SR	S	2	见A.2.13
18	失效日期	S	4	YYMM，见6.6
19	卡序列号	S	1	见A.2.14
20	卡保密号	D	1	见A.2.15
21	SAN-1	S	最大12	见A.2.16
22	字段分隔符	S	1	“=”，见6.4
23	SAN-2	S	最大12	见A.2.17
24	字段分隔符	S	1	“=”，见6.4
25	传递标志	S	1	见A.2.18
26	加密校验数	S	6	发卡机构自行规定，见A.2.19
27	附加数据	D	可变	见6.8
28	结束标志	S	1	“?”，见6.9
29	纵向冗余校验码	D	1	见GB/T15120.2

A.2 字段说明

A.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”（参见GB/T 2659）。

A.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：参见GB/T 12406。

A.2.3 金额指数

用途：决定周期授权量(A.2.4) 与本周期余额(A.2.5) 两字段的基值。

格式：1位数字。

内容：表示周期授权量(A.2.4) 与本周期余额(A.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。

A.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。

A.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(A.2.4)，消费后逐次递减，余额存本字段。

A.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。

A.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。

A.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。

A.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。

A.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。

A.2.11 主账号的账户类型(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：

第1位——账户类型

C——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。

第2位——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。

A.2.12 第1辅助账号的账户类型和服务约束

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

格式：2位数字。

内容：同 A.2.11。

A.2.13 第2辅助账号的账户类型和服务约束

用途：同A.2.11 中的定义一致，但此字段内容涉及第2辅助账号(SAN-2)(A.2.17) 中包含的账号。

格式：2位数字。

内容：同A.2.11。

A.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。

A.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出现在第3磁道上。

A.2.16 第1辅助账号(SAN-1)

用途：标明第1个可选用的辅助账号。

格式：最大12位数字。

内容：由发卡机构酌情使用。长度为0位数字时，表示不使用第1辅助账号。

A.2.17 第2辅助账号(SAN-2)

用途：标明第2个可选用的辅助账号。

格式：最大12位数字。

内容：由发卡机构酌情使用。长度为0位数字时，表示不使用第2辅助账号。

A.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位数字。

内容：

0——包括所有附加数据；

1——不包括附加数据；

2~9——无效。

A.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位数字。

内容：加密方法由各发卡机构自行规定。

附 录 B
(资料性附录)
卡片验证码(CVN) 的算法

CVN 的计算步骤如下:

计算CVN 时, 使用2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: 16位 PAN、4位卡失效日期和3位服务代码组成23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(Block)。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1组3位数即为CVN 值。

示例:

主账号: 6228888888888888 KeyA:0123456789ABCDEF

有效期: 1010 KeyB:FEDC BA9876543210

服务代码: 101

第1步: 数据源为62288888888888881010101

第2步: 扩展为62288888888888881010101000000000

第3步: Block1=6228888888888888

Block2=1010101000000000

第4步: 用KeyA对Block1加密; 结果为: C5736F4391690290

第5步: 将结果与 Block2异或, 结果为: D5637F5391690290; 再用KeyA加密, 结果为: 7D718A089D3ED5F9

第6步: 用KeyB解密, 结果为: 635205BF 4B97 EFB1

第7步: 用KeyA加密, 结果为: 4A4A 421A D41C 0319

第8步: 抽出结果中的数字, 结果为: 44421410319

第9步: 抽出结果中的字符, 结果为: AAAD C

减10后, 结果为: 00032

连接到第8步的结果之后为: 4442141031900032

第10步: 最左边三位数就是CVN=444。

附 录 C
(资料性附录)
PIN 验证码(PVN) 的算法

发卡机构使用至多16个128位PVN 加/解密密钥，在不同卡种中选择使用，每个密钥的索引号为0~F 之间的某个数值，随同密钥一起存放在加密机中。

PVN 的计算步骤如下：

- 1) 取双方约定的某个128位长的密钥Key,Key 的左侧64位为KeyA, 右侧64位为KeyB。
- 2) 取主账号右端除校验位以外的11位数字、密钥Key 的索引号I、PIN明文左端4位数字，依次构成一个16位数字串，每位数字用压缩BCD码表示，形成1个64位长的二进制计算块 Block。
- 3) 用KeyA 对 Block 做加密运算，得到结果Block1。
- 4) 用 KeyB 对 Block1 做解密运算，得到结果Block2。
- 5) 用 KeyA 对 Block2 做加密运算，得到结果 Block3。
- 6) 从左到右抽取出Block3 中所有的数字(0~9)。
- 7) 从左到右抽取出Block3 所有的十六进制字符(A~F)，并对每一个十六进制字符减十进制10，使之变为数字。
- 8) 将步骤6和7得出的数字依次从左至右排列，步骤7得出的数字放在步骤6得出的数字之后。
- 9) 取步骤8结果的前4位数字，即为PVN。

示例：

主账号 PAN=6228888888888888

密钥Key=0123456789AB CDEF FEDC BA9876543210

密钥索引号I=3

个人识别码PIN=123456

第1步：

KeyA=0123456789AB CDEF

KeyB=FEDC BA9876543210

第2步：

Block=8888888888831234 (注：实际运算中无需空格)

第3步：

Block1=DES(Encrypt,Block,KeyA)=573F 946B FDDE DCB3

第4步：

Block2=DES(Decrypt,Block1,KeyB)=D502 CA5A D7ED CD34

第5步：

Block3=DES(Encrypt,Block2,KeyA)=CB51 EB697ABD CB1C

第6步：

抽取Block3中的数字=516971

第7步：

抽取 Block3中的十六进制字符(CB EBAB DCBC),并作数值化处理=2141013212

第8步：

组合第6步和第7步=5169712141013212

第9步：

取第8步的前4位数字，PVN=5169

参 考 文 献

- [1]GB/T 17552—2008 信息技术识别卡金融交易卡(ISO/IEC 7813:2006,IDT)
[2]ISO 4909:2006 识别卡金融交易卡磁条第3磁道数据内容
-