ICS 点击此处添加 ICS 号
点击此处添加中国标准文献分类号

DB

北　京　市　地　方　标　准

DB XX/ XXXXX—XXXX

市政交通一卡通技术规范
第 2 部分：卡片规范

Municipal Administration & Communication Card Technology Standard

Part2：IC card

（征求意见稿）

XXXX - XX - XX 发布　　XXXX - XX - XX 实施

北京市质量技术监督局　发布

目　　次

前　言

DBxxxx-xxxx-《市政交通一卡通技术规范》分为五个部分：

---- 第1部分：总则；

---- 第2部分：卡片规范；

---- 第3部分：终端规范；

---- 第4部分：安全规范；

---- 第5部分：检测规范；

本部分为规范的第2部分。

本部分按照GB/T 1.1-2009给出的规则起草

本部分代替了DB11/T 159.1-2002《市政交通一卡通技术标准第1部分：卡片》，除编辑性修改外主要技术变化如下：

1.1. ----规范性引用文件中主要增加：“CJ/T 166 建设事业集成电路(IC)卡应用技术”、“GB/T22467.3 防伪材料通用技术条件 第3部分：防伪膜”两个规范及管理规定；规范性引用文件中删除：“GB/T 2260 中华人民共和国行政区划代码”、“GB/T 191 包装储运图示标志(eqv ISO 780)”、“GB/T 4754 国家经济行业分类与代码”三个规范及其管理规定。

----术语定义中增加；加密算法新技术术语定义、新型卡片种类的术语定义以及卡片防攻击术语定义。

----对“卡片规范”章节进行调整，增加芯片规范章节，规定了芯片容量要求以及芯片的性能指标等；增加了卡片规范章节，规定了卡片的物理、电器特性以及防伪要求；增加操作系统规范章节，规定了操作系统中掩膜要求等；增加卡片应用章节，引入了平台卡和异形卡等新的概念，规定了平台卡的基本要求。对“卡片规范”章节进行调整，删除逻辑加密卡相关内容。

----对“卡的安全机制”章节进行调整，增加对称算法、非对称算法、卡片防攻击内容。

----对“卡的安全机制”章节进行调整，将部分内容移至本标准的第4部分“安全规范”中。

----将“卡片检验方法”、“卡的验收规则”章节移至本标准的第5部分“检测规范”中。

本部分由北京市交通委员会提出并归口。

本部分由北京市交通委员会组织实施。

本部分主要起草单位：北京市交通信息中心、一卡通公司。

本部分主要起草人员：

引　　言

本部分为DBxxxx-xxxx的第2部分，与DBxxxx-xxxx的第1部分、第3部分、第4部分、和第5部分一起构成《市政交通一卡通技术规范》。

市政交通一卡通技术规范

第 2 部分：卡片规范

1 范围

本部分规定了市政交通一卡通系统集成电路（IC）卡（以下简称 IC 卡）的卡片技术要求和应用规范。

本部分适用于北京市政交通一卡通系统所使用的智能卡的设计、制造、管理、发行和应用。

2 规范性引用文件

下列文件中的条款通过本部分的引用而成为本部分的条款。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，鼓励根据本部分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部分。

GB/T 191　包装储运图示标志(eqv ISO 780:1997)

GB/T 13384　机电产品包装通用技术条件

GB/T 14916　识别卡　物理特性

GB/T 15120.1　识别卡-记录技术 第 1 部分：凸印

GB/T 16649.1　识别卡 带触点的集成电路卡 第 1 部分:物理特性

GB/T 17554　识别卡 测试方法

GB/T 22467.3　防伪材料通用技术条件 第 3 部分：防伪膜

JR/T 0025　中国金融集成电路（IC）卡规范

CJ/T 166　建设事业集成电路(IC)卡应用技术

ISO/IEC 14443-1　识别卡-无触点集成电路卡-邻近卡，第 1 部分：物理特性

ISO/IEC 14443-2　识别卡-无触点集成电路卡-邻近卡，第 2 部分：射频功率及信号接口

ISO/IEC 9798 信息技术-安全技术-实体鉴别

3 术语和定义

本部分采用以下术语和定义。

3.1

集成电路 Intergrated Circuit（s）（IC）
用于执行处理和/或存储功能的电子器件。

3.2

智能卡 Smart Card
带CPU的集成电路卡。

3.3

无触点IC卡Contactless Card
在卡内部封装一个集成电路和简单的天线，卡内无电池，用射频方式与外部集成电路进行耦合操作的IC卡。

3.4

一卡通卡 Multi-application Card
由市政府授权、在国家IC卡注册中心注册的发卡机构统一发行，并符合本规范的IC卡。

3.5

卡读写器IC Card Reader
可以对IC卡进行数据交换的终端设备。

3.6

充值机Add-value Machine
可以对IC卡中电子钱包进行充值的终端设备。

3.7

初始化Initialization
在卡发行前，由卡的发行机构对IC卡进行格式化，并在卡中写入卡的发行信息的过程。

3.8

应用文件Application File
按照一定的数据格式产生的具有不同功能的数据文件，无触点IC卡的应用文件包括卡的应用目录文件、发行文件、电子钱包文件、交易记录文件和用户过程文件等。

3.9

应用文件标识号Application File ID
按特定规则对每一个应用文件进行定义的文件号。

3.10

密码Password
相当于通行字或口令，当一方能向另一方提交出预先约定的密码时，提交一方的合法性才得以承认。

3.11

密钥Key
对数据进行加密时使用的秘密参数，经过加密后的数据文件称为密文，利用密钥可对密文解密，使原数据文件恢复。

3.12

电子钱包Electronic Purse

一种为方便持卡人进行小额消费而设计的IC卡应用，它支持圈存/消费等交易，除圈存交易外，其它任何交易均无须提交个人密码。

3.13

加密算法 Cryptographic Algorithm

为了隐藏或揭露信息内容而变换数据的算法。

3.14

明文 Plaintext

没有加密的信息。

3.15

密文 Ciphertext

通过密码系统产生的不可理解的文字或信号。

3.16

数字签名 Digital Signature

一种非对称加密数据变换，他使得接收方能够验证数据的原始性和完整性，保护发送和接受的数据不被第三方伪造，同时对于发送方来说，还可以防止接收方的伪造。

3.17

对称加密技术 Symmetric Cryptographic Technique

发送方和接收方使用相同保密密钥进行数据变换的加密技术，在不掌握保密密钥的情况下，不可能推导出发送方或者接收方的数据交换。

3.18

非对称加密技术 Asymmetric Cryptographic Technique

采用两种相关变换进行的加密技术，一种是公开变换（由公共密钥定义），另一种是私有变换（由私有密钥定义）。这两种变换具有以下属性，即私有变换不能通过给定的公开变换导出。

3.19

私钥 Private Key

一个实体的非对称密钥对中仅供实体自身使用的密钥，在数字签名模式中，私钥用于签名功能。

3.20

公钥 Public Key

一个实体的非对称密钥对中可以公开的密钥，在数字签名模式中，公钥用于验证功能。

3.21

非平台卡 Non Platform Card

智能卡COS与硬件平台紧密结合在一起，不具备二次开发能力的智能卡。

3.22

平台卡 Platform Card
智能卡具有安全防护性的方式来执行小型的Java Applet，这种智能卡称为平台卡。

3.23

标准卡 Standard Card
卡片规格遵循 GB/T 14916 5.1.1的尺寸和公差的卡片。

3.24

异形卡 Alien Card
卡片外观和尺寸不符合标准卡要求的卡片，也称之为异形卡或异型卡。

3.25

Inlay
封装的半成品测试样卡。

3.26

报文鉴别代码 Message Authentication Code
对交易数据及其相关参数进行运算后产生的代码。主要用于验证报文的完整性。

3.27

Timing攻击 Timing Attack
Timing 攻击，又叫时序攻击方法。在加密过程中，由于各分支语句的执行、频率、RAM命中率等因素所造成时间不一致。时序的攻击可以利用这些漏洞对系统进行攻击。

3.28

SPA/DPA攻击 Simple Power Analysis/Differential Power Analysis Attack
系统消耗功率的大小随微处理器执行的指令不同而不同。通过观察系统的功耗,来提取与密钥有关的信息，称之为SPA/DPA攻击。

4 缩略语

ADF 应用数据文件（Application Definition File）

AQL 合格质量水平（Acceptable Quality Level）

ATQA 对 A 型卡请求的应答（Answer To Request，Type A）

BCD 二-十进制编码（Binary Coded Decimal）

CPU 中央处理单元（Central Process Unit）

CSN 芯片序列号（Chip Serial Number）

EF　基本文件（Elementary File）

EP　电子钱包（Electronic purse）

HEX　十六进制数（Hexadecimal）

MAC　报文认证码（Message Authrntication Code）

MF　主文件（Master File）

NVM　非挥发性存储器（Nonvolatile memory）

PCD　接近耦合设备（Proximity Coupling Device）

POS　销售点终端（Point of Service）

SNR　序号（Serial Number）

5　芯片规范

5.1　芯片的一般特性要求

遵从 ISO/IEC14443 TYPE A 系列标准。

5.2　芯片的数据存储容量

芯片内 NVM 的数据容量应不小于 8Kbyte,并应具有足够存储空间，保留用于应用扩展。

5.3　芯片的使用寿命

芯片内 NVM 的擦写无故障次数应不少于 10 万次，数据存数保证 10 年不丢失。

5.4　微处理器及外围

处理器最低应为 8 位的低功耗微处理器，加密算法须采用硬件微处理器实现。

5.5　加密算法

数据的加密算法应支持对称加密算法或非对称加密算法。

5.6　安全特性

唯一序列号（UID）不可改写，写入的位置为 NVM 中的安全域，安全域应该有至少 16 字节预留。

注：NVM 中的安全域的区域只能写入一次的区域，一旦写入后不再支持更改，只具备读的属性。

5.7　数据总线加密

采用物理或逻辑方式加密等方法保护数据和程序代码。

5.8　抵抗电源干扰

自适应电路提供稳定的工作电源，高、低电压芯片复位。

5.9　频率保护

当芯片检测到频率不正常（过高或者过低），则芯片复位或者停止工作。

5.10 高射频场强保护

在高射频场强下，保证芯片不会被损坏。

5.11 抵抗反向工程

芯片出厂后无法再进入测试模式。只读存储 小器中的代码不可被外部程序或反向分析读出。

5.12 抗攻击

应采用抵抗非侵入式、半侵入式和侵入式攻击。

5.13 低功耗设计

智能卡低功耗应该从以下两个方面考虑：

a) 应采用低功耗工艺、器件。

b) 应采用低功耗电路、逻辑设计。

5.14 非接触通讯接口

非接触通讯接口遵循 ISO/IEC14443 TYPE A 系列标准。

6 卡片规范

6.1 卡片的一般特性要求

一卡通卡特性要求遵从 GB/T 14916 标准和 ISO/IEC14443 TYPE A 系列标准。

6.2 卡的标称尺寸

标准卡卡的标称尺寸应符合 GB/T 14916 中卡的标称尺寸的规定。

6.3 卡的表面

卡的表面应印制有“市政交通一卡通”字样和公司标识，卡面应压印卡的编号，压印的字符和位置应符合 GB/T 15120.1 的规定。

6.4 卡片防伪

卡的表面应增加北京市政交通一卡通专用防伪标识，防伪标识应符合 GB/T22467.3-2008 的规定。

6.5 卡的物理特性

6.5.1 动态弯曲特性

符合 ISO/IEC14443-1 中 4.3.3 的规定。

6.5.2 动态扭曲强度特性

符合 ISO/IEC14443-1 中 4.3.4 的规定。

6.5.3 卡的翘曲

符合 GB/T 14916 中 8.11 的规定。

6.5.4 耐温度

符合 GB/T 14916 中 8.12 的规定。

6.5.5 耐湿度

符合 GB/T 14916 中 8.5 的规定。

6.5.6 耐酸、 耐碱

符合 GB/T 14916 中 8.4 的规定。

6.5.7 紫外线

符合 ISO/IEC14443-1 中 4.3.1 的规定。

6.5.8 X 射线

符合 ISO/IEC14443-1 中 4.3.2 的规定。

6.5.9 静电

无触点 IC 卡符合 ISO/IEC14443-1 中 4.3.7 的规定。

带触点 IC 卡符合 GB/T 16649.1 中 4.2.8 的规定。

6.5.10 静磁场

符合 ISO/IEC14443-1 中 4.3.8 的规定。

6.5.11 交变磁场

符合 ISO/IEC14443-1 中 4.3.5 的规定。

6.5.12 交变电场

符合 ISO/IEC14443-1 中 4.3.6 的规定。

6.5.13 卡的负载调制振幅

用调试 PCD 组件对卡加 13.56MHz 载波和指令，卡负载调制振幅应符合 ISO/IEC14443-2 中 8.2.2 的规定。

6.6 卡的电气特性

6.6.1 卡的工作频率

卡的工作频率规定为 13.56 MHz±7 KHz。

6.6.2 卡的工作场强

即当 PCD 组件的激励频率为 13.56 MHz，场强最小为 1.5A/m 最大为 7.5A/m 时，卡应能正常应答。

6.6.3 通信速率

卡与读写器之间采用半双工通讯协议，其最低通信速率规定为 106k 波特率或 106k 波特率的倍频。

6.6.4 读写距离

卡与读写器之间感应距离在 0mm～100mm 应能正常通信。

6.7 卡的其它特性

6.7.1 复位应答

按本规范规定的通信协议和通信速率进行操作时，卡与读写器之间应能按 ISO/IEC14443-2 规定进行。

6.7.2 防冲突

卡片应具备防冲突能力。

7 操作系统规范

7.1 操作系统一般性要求

卡片操作系统须符合 JR/T 0025-2013 和 CJ/T 166-2006 的相关规定。

7.2 ATQA 响应时间要求

卡片在进入天线感应区后，ATQA 响应的时间须小于 3ms。

7.3 ATQA 返回数值要求

卡片采用 ATQA 返回值判别物理类型，返回值须为：0x0008。

7.4 掩膜要求

卡片操作系统须硬掩膜方式装载。

8 卡片应用

8.1 卡片形态

8.1.1 标准卡

卡片规格遵循 GB/T 14916 5.1.1 的尺寸和公差的卡片，称之为标准卡。

8.1.2 非标准卡

a) 异形卡

符合 GB/T 14916 规定的卡片厚度标准的，以标准非接触 IC 卡为基准，按照标准 IC 卡的封装工艺生产的，形状、外观不同于标准卡片的卡。

b) 异型卡

不符合 GB/T 14916 规定的卡片厚度标准的，含 IC 卡芯片的，可作为 IC 卡使用的复合材料卡片。

8.2 卡种划分

卡片按照操作系统的运行平台的不同可以分为非平台卡、平台卡

8.2.1 非平台卡

硬件规格：

a) 用户数据空间至少 8K 的 NVM。
b) 对称算法高速协处理器
c) PKI 协处理器

软件规格：

a) 符合 JR/T 0025-2013 和 CJ/T 166-2006 规范

8.2.2 平台卡

硬件规格：

a) 用户数据空间至少 200K
b) 低功耗芯片
c) 对称算法高速协处理器
d) PKI 协处理器

软件规格：

a) 符合 JR/T 0025-2013 和 CJ/T 166-2006 规范

8.3 卡片应用规划

8.3.1 卡结构

表1 智能卡的文件结构详细信息

文件名称	文件类型	文件存取控制	说明
MF			
DIR目录数据文件	记录文件	操作 = 安全认证	
发行基本信息文件	二进制文件	操作= 安全认证	
公共基本信息文件	二进制文件	操作= 安全认证	
交易记录文件	循环记录文件	操作= 安全认证	
金融应用			
公共应用基本数据文件	二进制文件	操作= 安全认证	
持卡人基本数据文件	二进制文件	操作= 安全认证	
交易明细文件	循环记录文件	读 = PIN保护，改写 = 不允许	
公交应用			
公共信息文件	二进制文件	操作= 安全认证	记录公交交易指针等信息
公交过程文件	循环记录文件	操作= 安全认证	记录持卡人乘坐公交车时的过程信息
专用卡信息文件	二进制文件	操作 = 安全认证	

专用钱包文件	钱包文件	操作= 安全认证	
轨道交通应用			
专用钱包信息文件	二进制文件	操作= 安全认证	
专用钱包文件	钱包文件	操作= 安全认证	
轨道交通过程文件	循环记录文件	操作= 安全认证	记录持卡人乘坐轨道交通工具时的过程信息

8.3.2 卡片中数据文件说明

8.3.2.1 MF 下应用文件说明

表2 MF 的发行基本信息说明

文件名称	发行基本信息文件
数据元	发行流水号
	卡的认证码
	卡类型
	发行版本
	发行日期（YYYYMMDD）
	失效日期（YYYYMMDD）

表3 MF 的公共基本信息说明

文件名称	公共基本信息文件
数据元	黑名单卡标志
	卡累计交易计数
	透支金额区
注：黑名单卡标志：0xA5－黑名单卡，0x00－正常卡	

8.3.2.2 金融应用区数据文件说明

金融应用下的文件、命令集、流程说明与 JR/T 0025 中的一致。

8.3.2.3 公交应用数据文件说明

表4 公交应用的专用信息文件说明

文件名称	公交应用的专用钱包信息文件
数据元	生效日期（YYMMDD）
	失效日期（YYMMDD）
	发行/充值机代码

8.3.2.4 轨道交通数据文件说明

表5 轨道交通应用的专用钱包信息文件说明

文件名称	轨道交通应用的专用钱包信息文件
数据元	生效日期（YYMMDD）
	失效日期（YYMMDD）
	发行/充值机代码

9 卡片安全机制

9.1 卡片算法

卡片需支持对称加密技术、非对称加密技术、安全哈希算法

9.1.1 对称加密技术

卡片须支持对称加密技术，具体算法标准参见 CJ/T 166-2006.

9.1.2 非对称加密技术

算法被用来进行静态数据和动态数据的验证以及数字签名。

在选择公开密钥模数长度时，应该考虑到密钥的生命周期以及在此生命周期内被解密的可能性。每个密钥的长度范围（上限、下限）在其相应的专用标准中规定。

发卡方公开密钥的指数的长度与IC卡公开密钥的指数长度由发卡方决定。

数字签名算法中的公开密钥算法的标志码为十六进制数字“01”。

9.1.3 安全哈希法

安全哈希算法参见 JR/T 0025-2013。

9.2 卡片通信安全

卡在交易过程中，为防止信号被意外截取，其数据通信均应加密，并按照 ISO/IEC9798 规定方法鉴别。

9.2.1 卡片密钥

城市公共交通IC卡规定一卡一密。卡的密钥利用卡的序列号（SNR）及其它有关信息，通过规定的加密算法，由卡的发行机构在对卡进行初始化时，记录在IC卡中。

卡片在每次写操作时，均需经过MAC验证，MAC的计算需要通过卡内密钥经过特定的计算方法计算得到。

9.2.2 卡片交易

卡片消费交易流程应满足交通行业的应用，金融应用应完全符合JR/T0025-2013消费交易；

卡片充值交易流程应满足交通行业的应用，金融应用应完全符合JR/T0025-2013中的圈存交易。

9.3 卡片防攻击

9.3.1 防 Timing 攻击

须能够抵御通过卡片 CPU 运算的时间差异分析卡片机密信息的攻击。

9.3.2 防 SPA/DPA 攻击

必须能够抵御卡片计算过程中能量消耗的变法而泄露卡片机密信息的攻击。

9.3.3 随机数产生器的随机性

卡片随机数的产生必须符合相关国家标准的随机性测试，确保随机数产生器的随机性符合安全要求。

10 包装、运输、贮存要求

10.1 包装

10.1.1 产品包装

产品包装应符合 GB/T 191 中的规定，并应符合 GB/T 13384-2008 中防潮、防霉的规定。

在包装箱上标志以下内容：

a) 产品名称、型号；
b) 制造厂厂名、厂址；
c) 外形尺寸及毛重；
d) “小心轻放”、“防潮”等字样相应图案；
e) 收货单位及地址；
f) 生产许可证编号。

10.1.2 包装箱

包装箱应有下列文件：

a) 装箱单；
b) 产品合格证；
c) 产品检测证书。

10.2 运输

由常规交通工具运输，在运输中必须防止受到强烈冲击、雨淋及曝晒。

10.3 贮存

应贮存于环境温度 0℃～40℃；相对湿度不大于 85% 的库房中，库房中不得有腐蚀性化学药品。