ICS 35.240.15
CCS L 64
备案号：108036-2024

DB11

北　京　市　地　方　标　准

DB11/T 159.2—2023
代替 DB11/T 159.2—2015

市政交通一卡通系统技术规范 第 2 部分：卡片

Technical specification for municipal administration & communications card system—Part 2：IC card

2023-12-25 发布　　2024-04-01 实施

北京市市场监督管理局　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

DB11/T 159《市政交通一卡通系统技术规范》分为以下部分：

——第1部分：总体要求；

——第2部分：卡片；

——第3部分：终端；

——第4部分：移动支付系统；

——第5部分：安全；

——第6部分：检测。

本文件是DB11/T 159的第2部分。

本文件代替DB11/T 159.2—2015《市政交通一卡通技术规范 第2部分：卡片》，与DB11/T 159.2—2015相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 更改了“数据存储容量”的要求（见5.2,2015年版的3.2）；
b) 更改了“卡片特性”规范性标准的要求（见第6章,2015年版的第4章）；
c) 更改了“封装”，删除了卡片封装防伪膜材料的要求（见7.1,2015年版的5.1）；
d) 增加了“印刷号”（见7.2），更改了“卡号编码”为“构成”（见7.2.1,2015年版的5.2.1）；更改了“卡号印刷”为“印刷”（见7.2.2,2015年版的5.2.2）；
e) 删除了“批次号印刷”（见2015年版的5.2.3）；
f) 更改了“操作系统规范”为“卡片指令”，并更改了“一般要求”相关标准的要求（见8.1,2015年版的6.1）；
g) 删除了“快速消费要求”（见2015年版的6.2.1）；
h) 增加了“算法”（见8.2.1）；
i) 增加了“算法区分”（见8.2.4）；
j) 更改了“卡种划分”统一为“卡片硬件规格要求”（见9.2,2015年版的7.2）；
k) 增加了“卡片典型交易时间”（见9.3）；
l) 更改了“卡结构”为“卡片数据结构”（见9.4.1,2015年版的7.3.1）；
m) 删除了“包装、运输、存储要求”（见2015年版本的第8章）。

本文件由北京市交通委员会提出并归口。

本文件由北京市交通委员会组织实施。

本文件起草单位：北京市智慧交通发展中心、北京市政交通一卡通有限公司、北京市标准化研究院。

本文件主要起草人员：隋莉颖、田旷、刘敬光、曾正喜、陈文革、周湘鹏、邢钊、郁国栋、罗琳、李佳霖、李强、杨雪、钟园、常新、葛启彬、马凌飞、许占富、李志宇、周巧霖、樊子风、蒋金煜、刘世俊、张腾、王海、李真丞、李昂、赵立华、金方伟、魏振阳。

本文件及其所代替文件的历次版本发布情况为：

——2002年首次发布DB11/T 159.1—2002《市政交通一卡通技术标准 第1部分：卡片》；

——2015年第一次修订时，将本文件改名为DB11/T 159.2—2015《市政交通一卡通技术规范 第2部分：卡片》；

——本次为第二次修订。

引　言

随着智慧城市建设的加速和公共交通的快速发展，市政交通一卡通系统在城市交通运营和民生服务中发挥着越来越重要的作用。为了提高城市公共交通运营效率和民生服务质量，满足市政交通一卡通系统的业务发展要求和民生服务需求，需要进行规范化的技术管理，北京市交通委员会组织编制了统一的技术标准。DB11/T 159《市政交通一卡通系统技术规范》由6个部分组成：

——第1部分：总体要求。目的在于明确市政交通一卡通系统的整体构成和要求。

——第2部分：卡片。目的在于明确市政交通一卡通系统卡片的要求。

——第3部分：终端。目的在于明确市政交通一卡通系统终端的要求。

——第4部分：移动支付系统。目的在于明确市政交通一卡通系统移动支付系统的组成和要求。

——第5部分：安全。目的在于明确市政交通一卡通系统安全的要求。

——第6部分：检测。目的在于明确市政交通一卡通系统检测的要求。

DB11/T 159《市政交通一卡通系统技术规范》参考了国家及地方的相关法规、行业标准和最佳实践，结合北京市公共交通行业特点和发展需求，以及新技术应用等进行了修订，保证标准具有先进性、安全性和指导性，保障市政交通一卡通系统长期、稳定和健康地发展。

DB11/T 159.2《市政交通一卡通系统技术规范 第2部分：卡片》涵盖了市政交通一卡通系统中卡片技术要求、卡片应用规范、卡片封装要求和卡片印刷要求等内容，适用于市政交通一卡通系统卡片设计、实施和运营。

市政交通一卡通系统技术规范
第 2 部分：卡片

1 范围

本文件规定了市政交通一卡通系统卡片的芯片要求、卡片特性、卡片封装、卡片指令和卡片应用的要求。

本文件适用于市政交通一卡通系统所使用的卡片设计、实施和运营。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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。

GB/T 14916 识别卡 物理特性

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 22351.1 识别卡 无触点的集成电路卡 邻近式卡 第1部分：物理特性

GB/T 22351.2 识别卡 无触点的集成电路卡 邻近式卡 第2部分：空中接口和初始化

JT/T 978.2 城市公共交通IC卡技术规范 第2部分：卡片

JT/T 978.5 城市公共交通IC卡技术规范 第5部分：非接触接口通信

JT/T 978.6 城市公共交通IC卡技术规范 第6部分：安全

DB11/T 159.1 市政交通一卡通系统技术规范 第1部分：总体要求

3 术语和定义

DB11/T 159.1界定的以及下列术语和定义适用于本文件。

3.1

卡片典型交易时间 card currently transaction time

完成一次从终端寻卡成功，到终端接收到卡片返回的最后一条指令的正常消费交易所消耗的卡片处理时间。

3.2

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。

[来源：JT/T 978.6—2015,3.3]

3.3

非对称加密技术 asymmetric cryptographic technique
采用公开变换（由公钥定义）和私有变换（由私钥定义）这两种相关变换的加密技术。
[来源：JT/T 978.6—2015,3.2]

3.4

标准卡 standard card
外观和尺寸符合 GB/T 14916 相关要求的卡片。

3.5

异形卡 alien card
外观和尺寸不符合 GB/T 14916 相关要求的卡片。

4 缩略语

DB11/T 159.1 界定的以及下列缩略语适用于本文件。
CLA：命令报文的类别字节(Class Byte of the Command Message)
DF：专用文件（Dedicated File）
FCI：文件控制信息（File Control Information）
INS：命令报文的指令字节（Instruction Byte of Command Message）
Lc:终端应用层命令中发出数据的实际长度
Le:响应数据中的最大期望长度
MAC:报文鉴别码（Message Authentication Code）
P1：参数 1（Parameter 1）
P2：参数 2（Parameter 2）
PKI：公开密钥基础设施（Public Key Infrastructure）
SM2:椭圆曲线公钥密码算法(Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves)
SM3：密码杂凑算法（SM3 Cryptographic Hash Algorithm）
SM4：分组密码算法（SM4 Cryptographic Algorithm）
SW1：状态字 1（Status Word One）
SW2：状态字 2（Status Word Two）

5 芯片要求

5.1 一般要求

应符合 JT/T 978.5 中 TYPE A 标准的相关要求。

5.2 数据存储容量

芯片内 NVM 的数据容量支持电子钱包应用的数据空间不应小于 20kB，支持电子现金应用的数据空间不应小于 10kB，并应预留足够存储空间，用于应用扩展。

5.3 使用寿命

芯片内 NVM 的擦写无故障次数不应少于 10 万次，数据存储应保证 10 年不丢失。

5.4 微处理器及外围

最低应为8位的低功耗微处理器，密码算法应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技术或非对称加密技术。

5.6 安全特性

CSN不应可改写。写入的位置为NVM中的安全存储空间，安全存储空间应有至少16Byte预留。

注：NVM中安全存储空间的区域只能写入一次，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

应采用物理或逻辑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，应支持高/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），应执行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，应保证芯片不会被损坏。

5.11 抵抗反向工程

芯片出厂后应无法再进入测试模式。只读存储器中的代码不能被读出或反向分析。

5.12 抗攻击

应能抵抗非侵入式、半侵入式和侵入式攻击。

5.13 低功耗设计

IC卡应采用低功耗工艺和器件；应采用低功耗电路和逻辑设计。

5.14 非接触通信接口

非接触通信接口应符合JT/T 978.5中TYPE A标准的相关要求。

5.15 掩膜方式

卡片操作系统应采用硬掩膜方式装载。

6 卡片特性

6.1 一般特性

应符合GB/T 14916和GB/T 22351的相关要求。

6.2 物理特性

6.2.1 动态弯曲特性

应符合 GB/T 22351.1 中的相关要求。

6.2.2 动态扭曲强度特性

应符合 GB/T 22351.1 中的相关要求。

6.2.3 翘曲

应符合 GB/T 14916 中的相关要求。

6.2.4 耐温度

应符合 GB/T 14916 中的相关要求。

6.2.5 耐湿度

应符合 GB/T 14916 中的相关要求。

6.2.6 耐酸、耐碱

应符合 GB/T 14916 中的相关要求。

6.2.7 紫外线

应符合 GB/T 22351.1 中的相关要求。

6.2.8 X 射线

应符合 GB/T 22351.1 中的相关要求。

6.2.9 静电

无触点 IC 卡应符合 GB/T 22351.1 中的相关要求。

带触点 IC 卡应符合 GB/T 16649.1 中的相关要求。

6.2.10 静磁场

应符合 GB/T 22351.1 中的相关要求。

6.2.11 交变磁场

应符合 GB/T 22351.1 中的相关要求。

6.2.12 交变电场

应符合 GB/T 22351.1 中的相关要求。

6.2.13 负载调制振幅

用调试 PCD 组件对卡片加 13.56MHz 载波和指令，卡片负载调制振幅应符合 GB/T 22351.2 中的相关要求。

6.3 电气特性

6.3.1 工作频率

卡片的工作频率应为 13.56MHz±7kHz。

6.3.2 工作场强

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

6.3.3 通信速率

卡片与读写器之间应采用半双工通信协议，其最低通信速率应为 106kbps 或 106kbps 的倍频。

6.3.4 读写距离

卡片与读写器之间感应距离在 0mm～100mm 应能正常通信。

6.4 其他特性

6.4.1 复位应答

按 6.3.3 中规定的通信协议和通信速率进行操作时，卡片与读写器之间应能按 GB/T 22351.2 中的相关要求进行复位应答。

6.4.2 防冲突

卡片应具备防冲突能力。

6.4.3 ATQA 响应时间要求

卡片在进入天线感应区后，ATQA 响应的时间应小于 3ms。

6.4.4 ATQA 返回数值要求

卡片应支持采用 ATQA 返回值判别物理类型，返回值应为：0x0008。

7 封装和印刷号要求

7.1 封装

卡片材质应为环保材料，耐高温，工作温度为-25℃～80℃。层压型工艺，采用覆盖膜。卡片表面光亮、整洁，无污渍和刮痕，不应有模块和天线的痕迹。耐磨损，不易变形，在有效使用期内不应发生分层和剥落现象。

卡片分层结构应遵照如图 1 所示：

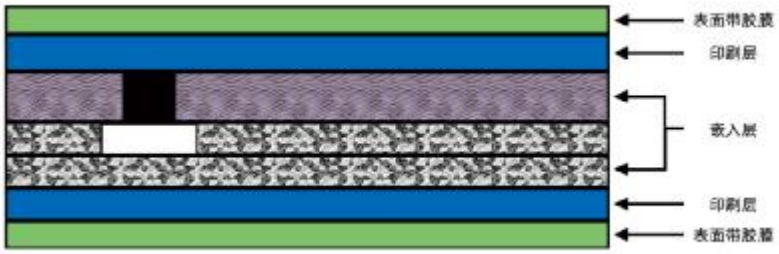

图 1　卡片分层结构图

7.2　印刷号

7.2.1　构成

印刷号应由 23 位数字组成。如下：

印刷号 = 发卡机构识别码（即 IIN 码） + 扩展发卡机构识别码 + 发行顺序号 + 校验位

310517 + 00 + xxxxxxxxxxx + xxxx，310517 为发卡机构识别码（即 IIN 码），00 为扩展发卡机构识别码，xxxxxxxxxxx 为 11 位卡片发行顺序号，xxxx 为 4 位校验位。

7.2.2　印刷

标准卡印刷要求如下：

3105 1700 xxxx xxxx xxx xxxx

说明：第四个字符和第五个字符之间有一个空格，第八个字符和和第九个字符之间有一个空格，第十二个字符和第十三个字符之间有一个空格，第十六个字符和第十七个字符之间有一个空格，第十九个字符后回车换行，4 位卡号校验位与卡片流水号右侧对齐。

印刷号应位于卡片正面，采用激光打印凹字的方式完成，打印印刷号总长 68.6mm，高 5.5mm，校验位总长 10mm，高 3.5mm。如图 2 中阴影部分为卡号打印区域，卡片的模块、线圈、触点和磁条不应放置在该区域内。

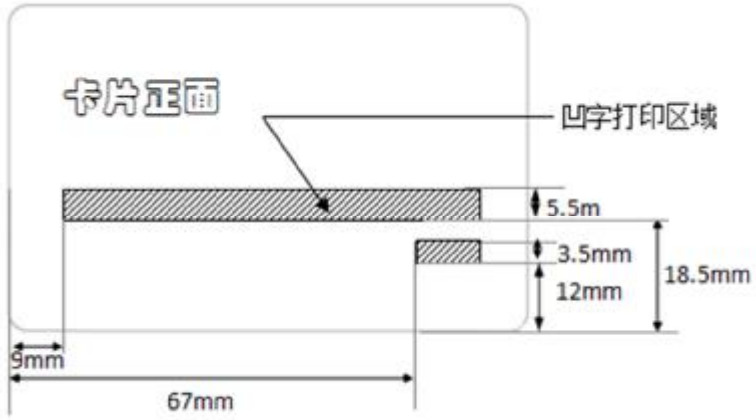

图2 印刷号位置示意图（2）

8　卡片指令

8.1 一般要求

卡片操作指令应满足 JT/T 978.2 的指令及应用规范的要求。

8.2 特殊要求

8.2.1 算法

卡片芯片应支持 SM2 或 SM3 或 SM4 算法。

卡片芯片同时支持多算法时，应满足算法切换和算法区分的要求。

8.2.2 算法切换

卡片支持两种算法时，应根据不同的密钥标识按要求进行算法切换，具体要求如下：

a) 算法切换指令对多算法卡片应具有以下四种功能：读取当前算法、算法选择、默认算法设定和算法锁定；
b) 支持两种或两种以上算法的卡片可装载多组多条算法密钥，应通过密钥标识符进行分组和区分；
c) 通过对卡片发送算法切换指令实现算法的选择，对于可输入密钥标识符的指令，密钥标识符所对应的算法应与当前所选择的算法一致，若不一致，应反馈错误信息。发送算法切换指令对后续指令中所使用的算法进行选择，所选算法在掉电情况下应恢复为默认算法；
d) 未接收到算法选择指令时，卡片应使用默认算法进行交易，默认算法可通过算法切换指令进行更改；
e) 算法应能够通过算法切换指令实现永久关闭或锁死。算法锁定指令应带 MAC 码，使用待锁定算法对应的密钥索引低半个字节为 1 的维护密钥计算 MAC。发送算法锁定指令时，应先使用算法切换指令将卡片的当前默认算法设置为非锁定的算法。

8.2.3 算法切换指令

算法切换指令格式如下：

a) 算法切换指令报文见表 1；

表1 算法切换指令报文

编码	值	说明
CLA	‘80/84’	当含安全报文MAC时使用84
INS	‘CD’	命令报文的指令字节
P1	XX	00：读取当前密钥组（当未选择密钥组时返回默认密钥组，否则为当前选择的密钥组，此时P2为00） 01：选择P2指定的密钥组别 02：设置P2指定的密钥组别为默认组别 03：锁定P2指定的密钥组别，此时Data域为4字节MAC值，CLA为84
P2	XX	密钥组别索引，当P1=00时 P2=00
Lc	XX	P1=00/01/02时 Lc=00 P1=03时 Lc=04
Data		P1=00/01/02时 Data不存在 P1=03时 Data=MAC(4字节)
Le	XX	P1=00时 Le=01 P1=01/02/03时 Le不存在

b) 算法切换指令数据域：当 P1=03 时，数据域为 4 字节 MAC 数据；当 P1 非 03 时，数据域不存在；
c) 算法切换指令响应数据域：当 P1=00 读取当前密钥组时，响应报文数据域为当前密钥组别；当 P1 非 00 时，响应报文数据域不存在；
d) 算法切换指令响应报文的状态码见表 2。

表2 算法切换指令响应报文的状态码

SW1	SW2	说明
90	00	正确执行
67	00	错误的长度
6A	86	P1、P2参数错误
6D	00	INS不支持或错误
6E	00	CLA不支持或错误
69	81	密钥与运算方法（密钥组算法）不匹配
69	82	不满足安全状态
69	83	密钥(组别)已被锁定
69	85	不满足使用条件
6A	82	KEY文件不存在
94	03	密钥(组别)不存在

8.2.4 算法区分

选择电子钱包应用时，在返回的 FCI 中应使用 DF00 标签，长度 1 字节，用于指示当前卡片支持的算法类型。响应报文见表 3。

表3 选择电子钱包应用的响应报文

标签	值（十六进制）			条件
6F	FCI模板			M
	84	DF名		M
	A5	FCI数据专用模板		M
		50	应用标签	O
		87	应用优先指示符	O
		9F08	应用版本号	M
		9F12	应用优先名称	O
		DF00	算法指示	M
		9F0C	发卡机构自定义数据	O
注：M-必备，O-可选				

8.2.5 算法操作指令

算法操作指令可指定当前流程使用算法类别，用于查询当前算法类别、指定当前流程使用的算法类别、切换默认密钥组和锁定指定密钥组。指令见表 4。

表4　算法操作指令

编码	值	说明
CLA	‘80/84’	当含安全报文MAC时使用84
INS	‘CD’	命令报文的指令字节
P1	XX	‘00’：读取当前密钥组（返回值：019000或039000） ‘01’：选择P2指定的密钥组别（成功返回9000） ‘02’：设置P2指定的密钥组别为默认组别（成功返回9000） ‘03’：锁定P2指定的密钥组别（成功返回9000）
P2	XX	P1=‘00’时：P2=00 P1=‘01’/‘02’/‘03’时：P2密钥组别索引
Lc	XX	当CLA=‘80’时，Lc为‘00’，00 01 02 当CLA=‘84’时，Lc为‘04’
Data		当P1=‘00’、‘01’、‘02’时，不存在数据域 当P1=‘03’时，4字节MAC值
Le	XX	P1=‘00’时：Le=01 P1=‘01’/‘02’/‘03’时：不存在

使用该指令的要求：

a) 当发送的指令带密钥索引时，应直接使用密钥索引来判断算法；

b) 当发送的指令不带密钥索引时，应使用算法操作指令指定算法。

9　卡片应用

9.1　卡片形态

卡片按形态不同可分成标准卡和异形卡。

9.2　卡片硬件规格要求

硬件规格应符合如下要求：

a) 采用低功耗芯片；

b) 采用对称算法高速协处理器；

c) 支持 PKI 算法的具备 PKI 协处理器。

9.3　卡片典型交易时间

正常消费交易，典型交易时间不应超过 300ms。

9.4　卡片应用信息

9.4.1　卡片数据结构

卡片基本应用数据结构信息见表 5。

表5　卡片数据结构信息

文件名称	文件类型	说明
电子钱包应用		
公共应用基本文件	二进制文件	
持卡人基本信息文件	二进制文件	
管理信息文件	二进制文件	
交易明细文件	记录文件	
公共交通过程信息变长记录文件	记录文件	包括城市轨道、公交汽电车和轮渡等应用记录，支持复合消费更新
公共交通过程信息循环记录文件	记录文件	支持复合消费更新
发行基本信息文件	记录文件	
过程信息文件	记录文件	包括城市轨道联乘积分等过程记录，支持复合消费更新
私有过程信息文件	记录文件	支持复合消费更新
实名照片文件	二进制文件	
电子现金应用		

9.4.2　卡片数据文件

9.4.2.1　公共应用基本文件

公共应用基本文件见表 6。

表6　公共应用基本文件

文件名称	公共应用基本文件
数据元	发卡机构标识
	应用类型标识
	发卡机构应用版本
	应用序列号
	应用启用日期
	应用失效日期
	发卡机构自定义 FCI 数据

9.4.2.2　管理信息文件

管理信息文件见表 7。

表7　管理信息文件

文件名称	管理信息文件
数据元	国际代码
	省级代码
	城市代码
	互通卡种
	卡种类型

9.4.2.3 城市轨道应用信息记录文件

城市轨道应用信息记录文件见表 8。

表8 城市轨道应用信息记录文件

文件名称	城市轨道应用信息记录
数据元	记录 ID 标识
	记录长度
	应用有效标识
	互联互通交易标识
	应用锁定标志
	交易流水号
	交易状态
	进闸城市代码
	出闸城市代码
	进闸城市机构标识
	出闸城市机构标识
	进闸线路号
	出闸线路号
	进闸站点
	出闸站点
	进闸终端编号
	出闸终端编号
	进闸时间
	出闸时间
	进闸交易金额
	进闸钱包金额
	出闸交易金额
	最大消费金额

9.4.2.4 公共汽电车应用信息记录文件

公共汽电车应用信息记录文件见表 9。

表9 公共汽电车应用信息记录文件

文件名称	公共汽电车应用信息记录
数据元	记录 ID 标识
	记录长度
	互联互通交易标识
	应用锁定标志
	交易流水号
	交易状态

表 9　公共汽电车应用信息记录文件（续）

文件名称	公共汽电车应用信息记录
	上车城市代码
	下车城市代码
	上车机构标识
	下车机构标识
	上车站点
	下车站点
	上车终端编号
	下车终端编号
	上车时间
	下车时间
	最大消费金额
	方向标识
	线路号
	车辆号

9.4.2.5　停车收费应用信息记录文件

停车收费应用信息记录文件见表10。

表10　停车收费应用信息记录文件

文件名称	停车收费应用信息记录
数据元	记录 ID 标识
	记录长度
	日期时间（到达/离开）
	状态码
	停车场编号

9.4.2.6　积分应用信息记录文件

积分应用信息记录文件见表11。

表11　积分应用信息记录文件

文件名称	积分应用信息记录
数据元	记录 ID 标识
	记录长度
	联乘信息
	累积开始时间
	累积金额（次数）

9.4.2.7　基本信息文件

基本信息文件见表12。

表12　基本信息文件

文件名称	基本信息文件
数据元	信息加密方式
	行业内标识
	人员信息
	证件号码
	证件类型

9.4.2.8　照片存储文件

照片存储文件见表13。

表13　照片存储文件

文件名称	照片存储文件
数据元	照片长度
	照片二进制数据

9.4.2.9　电子现金应用区数据文件

电子现金应用下的文件、命令集和流程应符合 JT/T 978.2 的相关要求。