ICS 35.240.15
L 64

DB11

北　京　市　地　方　标　准

DB11/T 159.2—2015
代替 DB11/T 159.2—2005

市政交通一卡通技术规范
第 2 部分：卡片

Municipal administration & communication card technology specifications—Part 2:IC card

2015－01－28 发布　　2015－08－01 实施

北京市质量技术监督局　发布

目　　次

前　言

本部分按照GB/T 1.1-2009给出的规则起草

DB11/T 159《市政交通一卡通技术规范》分为5个部分：

---- 第1部分：总则；

---- 第2部分：卡片；

---- 第3部分：终端；

---- 第4部分：安全；

---- 第5部分：检测。

本部分为DB11/T 159的第2部分。

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》。

本部分与DB11/T 159.1-2002相比主要变化如下：

——修改了前言的描述（见前言，2002年版的前言）；

——删除了引言（见2002年版的引言）；

——修改了规范性引用文件清单所列标准中标示与引用文件的对应关系，只有正在起草的与引用文件存在一致性程度的标准，才需标示（见2，2002年版的2）；

——对“术语和定义”及“符号和缩略语”在正文中的出现情况做了核对，删除了没有出现的，修改了出现的，并同步将术语定义和缩略语统一在本标准第1部分“总则”中定义（见本标准第1部分的3和4，2002年版的3和4）；

——删除了“卡片规范”，调整为“芯片特性”（增加了芯片容量要求以及芯片的性能指标等）、“卡片特性”（增加了卡片的物理、电器特性以及防伪要求）、“卡片应用”（增加了平台卡和异形卡要求），删除了逻辑加密卡相关内容（见3、4和7，2002年版的5）；

——增加了“卡片封装”（见5）；

——增加了“操作系统规范”（见6）；

——删除了“卡的安全机制”，将内容移至本标准的第4部分“安全”中（见2002年版的6）；

——删除 “卡片检验方法”、 “卡的验收规则”移至本标准的第5部分“检测”中（见2002年版的7和8）。

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、北京市政交通一卡通有限公司。

本部分主要起草人员：陈文革、曾正喜、周湘鹏、蒋金煜、邢钊、白洪波、刘敬光、卢明、葛昱、邹迎、李倩、陈智宏、刘浩、隋莉颖、王立勋、李伟。

市政交通一卡通技术规范

第 2 部分：卡片

1 范围

本部分规定了市政交通一卡通卡片的技术要求，包括芯片特性、卡片特性、卡片封装、操作系统规范、卡片应用、包装、运输和贮存的要求。

本部分适用于市政交通一卡通系统所使用的智能 IC 卡设计、制造、管理、发行和应用。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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 191 包装储运图示标志

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

CJ/T 304 建设事业 CPU 卡操作系统技术要求

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 芯片特性

3.1 一般特性

应执行 ISO/IEC14443 TYPE A 系列标准。

3.2 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。

3.3 使用寿命

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

3.4 微处理器及外围

处理器最低应为 8 位的低功耗微处理器，加密算法应采用硬件微处理器实现。

3.5 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。

3.6 安全特性

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

注：NVM 中安全域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。

3.7 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。

3.8 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。

3.9 频率保护

当芯片检测到频率不正常（过高或者过低），应芯片复位或者停止工作。

3.10 高射频场强保护

在高射频场强下，应保证芯片不会被损坏。

3.11 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外部程序或反向分析读出。

3.12 抗攻击

应采用抵抗非侵入式、半侵入式和侵入式攻击。

3.13 低功耗设计

智能卡低功耗应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。

3.14 非接触通信接口

非接触通信接口遵循 ISO/IEC14443 TYPE A 系列标准。

3.15 掩膜要求

卡片操作系统应采用硬掩膜方式装载。

4 卡片特性

4.1 一般特性

应执行 GB/T 14916 标准和 ISO/IEC 14443 TYPE A 系列标准。

4.2 物理特性

4.2.1 动态弯曲特性

应符合 ISO/IEC 14443-1-1997 中 4.3.3 的规定。

4.2.2 动态扭曲强度特性

应符合 ISO/IEC 14443-1-1997 中 4.3.4 的规定。

4.2.3 翘曲

应符合 GB/T 14916-2006 中 8.11 的规定。

4.2.4 耐温度

应符合 GB/T 14916-2006 中 8.12 的规定。

4.2.5 耐湿度

应符合 GB/T 14916-2006 中 8.5 的规定。

4.2.6 耐酸、耐碱

应符合 GB/T 14916-2006 中 8.4 的规定。

4.2.7 紫外线

应符合 ISO/IEC 14443-1-1997 中 4.3.1 的规定。

4.2.8 X 射线

应符合 ISO/IEC 14443-1-1997 中 4.3.2 的规定。

4.2.9 静电

无触点 IC 卡应符合 ISO/IEC 14443-1-1997 中 4.3.7 的规定。

带触点 IC 卡应符合 GB/T 16649.1-2006 中 4.2.8 的规定。

4.2.10 静磁场

应符合 ISO/IEC 14443-1-1997 中 4.3.8 的规定。

4.2.11 交变磁场

应符合 ISO/IEC 14443-1-1997 中 4.3.5 的规定。

4.2.12 交变电场

应符合 ISO/IEC 14443-1-1997 中 4.3.6 的规定。

4.2.13 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/IEC 14443-2-1999 中 8.2.2 的规定。

4.3 电气特性

4.3.1 工作频率

卡的工作频率应为 13.56 MHz±7 KHz。

4.3.2 工作场强

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。

4.3.3 通信速率

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

4.3.4 读写距离

标准卡与读写器之间感应距离在(0～100)mm 应能正常通信。

异形卡与读写器之间感应距离在(0～60)mm 应能正常通信。

4.4 其它特性

4.4.1 复位应答

按本标准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/IEC 14443-2 规定进行复位应答。

4.4.2 防冲突

卡片应具备防冲突能力。

4.4.3 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。

4.4.4 ATQA 返回数值要求

卡片采用 ATQA 返回值判别物理类型，返回值应为：0x0008。

5 卡片封装

5.1 封装要求

卡基材质应为优质环保材料，耐高温，工作温度为-25℃~80℃。层压型工艺，采用优质覆盖膜。卡片表面光亮、整洁，无污渍、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、剥落现象。

应在卡片指定位置封装定制的光学防伪膜材料，不影响卡片的封装质量。

卡片封装应遵照如图 1 所示：

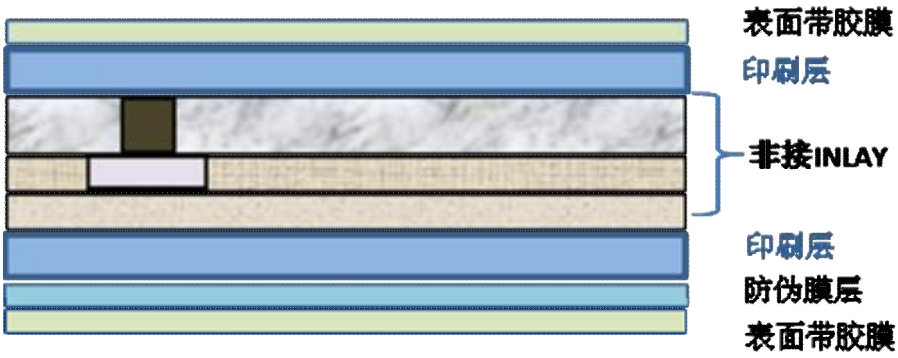

图 1　卡体分层结构图

5.2　印刷要求

5.2.1　卡号编码

卡片应印刷编号，编号由 20 位数字组成。如下：

AAAABBBBBBBBBBBBCCCC，A 为城市编码，B 为卡发行顺序号，C 为卡校验位。

符合 GB/T 14916-2006 中 5.1.1 的卡片，编号印刷应按本部分的 5.2.2、5.2.3 规定执行。

不符合 GB/T 14916-2006 中 5.1.1 的卡片，编号印刷格式可根据卡片形态调整。

5.2.2　卡号印刷

符合 GB/T 14916-2006 中 5.1.1 的尺寸和公差卡片的印刷编号由 20 位数字组成。如下：

AAAABBBB BBBBBBBB CCCC

说明：第八个字符和第九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。

卡号应位于卡片正面，字体应为 Romans（此字体与 Microsoft Office Word 内的 Romans 字体一致），采用激光打印凹字的方式完成，打印卡号总长 45.5mm，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、触点和磁条不能放置在该区域内。

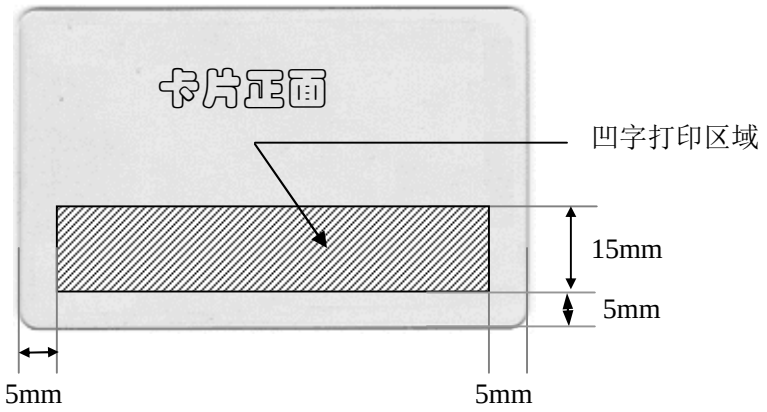

图 2　卡号位置示意图

5.2.3 批次号印刷

卡面批次号印刷应在每张卡片背面的左下角，字体为 Arial 6.8 磅，采用平印的方式执行。如图 3 中阴影部分为批次号打印区域。

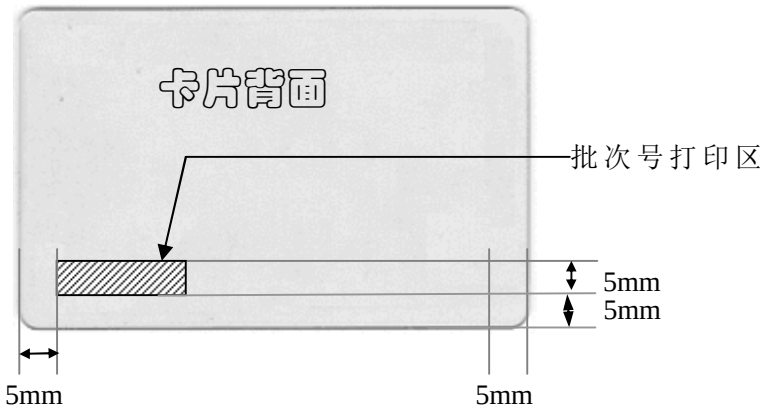

图 3　批次号位置示意图

6 操作系统规范

6.1 一般性要求

卡片操作系统应符合 CJ/T 304 和 CJ/T 166 的相关规定，支持电子现金应用时应符合 JR/T 0025 的相关规定。

6.2 特殊性要求

6.2.1 快速消费

6.2.1.1 快速消费要求

快速消费交易指令分为预消费指令和消费数据归位指令。

快速消费交易应在 40ms 内完成。在预消费指令执行时，将生成的 TAC，MAC，交易明细，余额，状态信息等信息拼装成一个数据块，一次性写入 NVM 中定义好的区域中(注意：这时并不将真实数据写入钱包和卡记录等位置)，同时标识真实数据没有归位的标志，然后返回 TAC+MAC，完成预消费。真实数据归位可在其它时间段完成。

指令中的 MAC1、TAC、MAC2 的算法与 CJ/T 304-2008 中的第 9 章的电子存折/电子钱包应用所定义的保持一致。交易流程参见 CJ/T 304-2008 中的 9.4.4 节，将其中的 Debit for Purchase 指令替换成预消费指令。快速消费数据归位指令可在流程外发送给卡片。为保持钱包数据的正确性，COS 应在任何关于钱包操作的指令前先检查快速消费数据归位标志，若没有归位，应先归位钱包数据然后才响应新的钱包操作指令。

6.2.1.2 预消费指令

预消费指令要求如下：

a) 预消费指令报文见表 1。

表1　预消费指令报文

代码	长度（byte）	值（HEX）	描述
CLA	1	80	—
INS	1	54	—
P1	1	05	此处为预消费标识，其它与CJ/T 304-2008 中9.3.5一致
P2	1	00	—
Lc	1	0F	—
DATA	15	XX…XX	见下面的命令报文数据域
Le	1	08	

b)　预消费指令数据域见表 2。

表2　预消费指令数据域

说明	长度（byte）
终端交易序号	4
交易日期（终端）	4
交易时间（终端）	3
MAC1	4

c)　预消费响应报文数据域见表 3。

表3　预消费响应报文数据域

说明	长度（byte）
交易验证码TAC	4
MAC2	4

d)　预消费响应报文的状态码见表 4。

表4　预消费响应报文的状态码

SW1	SW2	说明
‘65’	‘81’	内存错误
‘67’	‘00’	长度错误
‘69’	‘01’	命令不接受（无效状态）
‘69’	‘85’	使用条件不满足
‘6D’	‘00’	INS不支持或错误
‘6E’	‘00’	CLA不支持或错误
‘93’	‘02’	MAC无效

6.2.1.3　消费数据归位指令

消费数据归位指令要求如下：

a)　消费数据归位指令报文见表 5。

表5　消费数据归位指令报文

代码	长度（byte）	值（HEX）	描述
CLA	1	80	—
INS	1	54	—
P1	1	06	此处为消费标识，
P2	1	00	—
Lc	1	00	—

b)　消费数据归位响应报文的状态码见表 6。

表6　消费数据归位响应报文的状态码

SW1	SW2	说明
‘65’	‘81’	内存错误
‘67’	‘00’	长度错误
‘69’	‘01’	命令不接受（无效状态）
‘69’	‘85’	使用条件不满足
‘6D’	‘00’	INS不支持或错误
‘6E’	‘00’	CLA不支持或错误
‘90’	‘00’	成功

6.2.2　算法切换

6.2.2.1　算法切换要求

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)　算法切换指令对双算法卡片具有以下四种功能：读取当前算法、算法选择、默认算法设定、算法锁定；

b)　支持两种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)　不发送算法选择指令时，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双算法卡片的当前默认算法设置为非锁定的算法。

6.2.2.2　算法切换指令

算法切换指令要求如下：

a)　算法切换指令报文见表 7；

表7　算法切换指令报文

代码	值	说明
CLA	‘80/84’	当含安全报文MAC时使用84
INS	‘CD’	
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（01：DES/3DES；02：预留；03：SM4；04：预留），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 8。

表8　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

7　卡片应用

7.1　卡片形态

卡片按形态不同可分成标准卡和异形卡。

7.2 卡种划分

7.2.1 非平台卡

硬件规格要求如下：

a) 用户数据空间应不少于 8Kbyte 的 NVM；
b) 应采用对称算法高速协处理器；
c) 支持 PKI 算法的应具备 PKI 协处理器。

软件规格应符合 CJ/T 304 和 CJ/T 166 的要求，支持电子现金应用时应符合 JR/T 0025 的要求。

7.2.2 平台卡

硬件规格要求如下：

a) 用户数据空间应不少于 40Kbyte 的 NVM；
b) 应采用低功耗芯片；
c) 应采用对称算法高速协处理器；
d) 支持 PKI 算法的应具备 PKI 协处理器。

软件规格应符合 CJ/T 304 和 CJ/T 166 的要求，支持电子现金应用时应符合 JR/T 0025 的要求。

7.3 卡片应用信息

7.3.1 卡结构

卡片基本应用结构信息见表9。

表9 卡结构信息

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	
公共电汽车应用			
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
公共电汽车过程文件	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	

表 9 卡结构信息（续）

文件名称	文件类型	文件存取控制	说明
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
停车场应用			
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	
停车场过程文件	循环记录文件	操作= 安全认证	记录持卡人进出停车场时的过程信息
自行车租赁			
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	
自行车租赁过程文件	循环记录文件	操作= 安全认证	记录持卡人租赁自行车时的过程信息

7.3.2 卡片数据文件说明

7.3.2.1 MF 基本应用文件

卡片MF下发行基本信息见表10，公共基本信息见表11。

表10 MF 的发行基本信息

文件名称	发行基本信息文件
数据元	发行流水号
	卡类型
	卡状态
	发行版本
	卡的认证码
	发行日期（YYYYMMDD）
	失效日期（YYYYMMDD）
	国家注册发行号
	证件编号
	证件类型
	预留

表11 MF 的公共基本信息

文件名称	公共基本信息文件
数据元	透支金额区
	卡累计交易计数
	黑名单卡标志
	联乘优惠标志
	联乘开始时间(YYMMDDhhmm)

表 11 MF 的公共基本信息（续）

文件名称	公共基本信息文件
	联乘开始线路
	联乘开始站号
	预留

7.3.2.2 金融应用区数据文件

金融应用下的文件、命令集、流程应与 JR/T 0025 的要求一致。

7.3.2.3 公共电汽车应用数据文件

公共电汽车应用基本信息见表12。

表12 公共电汽车应用基本信息

文件名称	公共电汽车应用基本信息文件
数据元	上车时间(YYMMDDhhmm)
	下车时间(YYMMDDhhmm)
	上车站标
	下车站标
	方向标识
	标注金额
	线路号
	车辆号
	预留

7.3.2.4 轨道交通数据文件

轨道交通应用基本信息见表13。

表13 轨道交通应用基本信息

文件名称	轨道交通应用基本信息文件
数据元	入口时间(YYMMDDhhmm)
	入口线路码
	入口站码
	入口时钱包余额
	标注金额/联乘累计金额
	出口时间(YYMMDDhhmm)
	出口线路码
	出口站码
	联乘开始时间(YYMMDDhhmm)
	联乘开始线路码
	联乘开始站码
	预留

7.3.2.5 停车场数据文件

停车场应用基本信息见表14。

表14 停车场应用基本信息

文件名称	停车场应用基本信息文件
数据元	停车场编号
	入场站台
	入场时间(YYMMDDhhmm)
	出场站台
	出场时间(YYMMDDhhmm)
	预留

7.3.2.6 自行车租赁数据文件

自行车租赁应用基本信息见表15。

表15 自行车租赁应用基本信息

文件名称	自行车租赁应用基本信息文件
数据元	取车终端号
	还车终端号
	取车时间(YYMMDDhhmm)
	还车时间(YYMMDDhhmm)
	车辆号
	交易金额
	欠费金额
	预留

8 包装、运输、贮存要求

8.1 包装

8.1.1 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。

在包装箱上应标志以下内容：

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。

8.1.2 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。

8.2 运输

在运输中应防止受到强烈冲击、雨淋及曝晒。

8.3 贮存

应贮存于环境温度 0℃～40℃，相对湿度不大于 85% 的库房中，库房中不应有腐蚀性、放射性等危险品。