ICS 35.240.15

|  |
| --- |
| L 64备案号： |

|  |
| --- |
|  |

DB11

北京市地方标准

DB11/T 159.4—20xx

|  |
| --- |
| 代替 DB11/T 159.4—2015 |

DB11/T 159.4—20XX

|  |
| --- |
| DB11/T 159.4—20XX |

市政交通一卡通技术规范

第4部分：安全

Municipal administration & communication card technology specifications—Part 4:Security

|  |
| --- |
|  |
|  |

20XX - XX - XX发布

20XX - XX - XX实施

北京市市场监督管理局   发布

目  次

前言 III

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 缩略语 3

5 卡片安全 4

5.1 一般性要求 4

5.2 共存应用 4

5.3 密钥的独立性 4

5.4 卡片内部安全体系 4

5.5 卡片通信安全 7

5.6 卡片交易安全 7

5.7 卡片防攻击 7

5.8 卡片国密算法要求 7

6 终端安全 7

6.1 终端数据安全 7

6.2 终端设备安全 8

6.3 终端密码算法要求 8

7 系统安全 8

7.1 通用要求 8

7.2 安全物理环境 9

7.3 安全通信网络 9

7.4 安全区域边界 9

7.5 安全计算环境 9

7.6 安全管理中心 10

7.7 云计算扩展要求 11

7.8 移动互联扩展要求 11

7.9 移动支付系统安全要求 11

8 交易安全 11

8.1 消费类交易安全 12

8.2 充值类交易安全 12

8.3 退卡类交易安全 12

9 密钥管理及算法 13

9.1 通用要求 13

9.2 生成与发行 13

9.3 安全机制 14

9.4 密钥算法 14

9.5 国密算法对称加密机制 14

9.6 国密算法非对称加密机制 15

附录A（规范性）MAC计算—DEA算法 16

附录B（规范性）MAC计算—SM4算法 17

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。

本文件是DB11/T 159《市政交通一卡通技术规范》的第4部分。DB11/T 159 已经发布了以下部分：

——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；

——第6部分：移动支付。

本文件代替DB11/T 159.4—2015《市政交通一卡通技术标准第4部分：安全》，与DB11/T 159.4—2015相比，除结构调整和编辑性改动外，主要技术变化如下：

1. 增加了安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、云计算安全扩展要求、移动互联安全扩展要求（见7）；
2. 增加了“移动支付系统安全要求”章节（见7.9）；
3. 增加了卡片国密算法的相关要求（见5.8）；
4. 增加了终端国密算法的相关要求（见6.3）；
5. 增加了SM2/3/4国密算法的相关描述（见9.4）。

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。

本文件主要起草单位：北京市智慧交通发展中心、北京市政交通一卡通有限公司。

本文件主要起草人员：

本文件及其所代替文件的历次版本发布情况为：

——2015年首次发布DB11/T159.4—2015《市政交通一卡通技术规范 第4部分：安全》;

——本次为第一次修订。

市政交通一卡通技术规范

第4部分：安全

1. 范围

本文件规定了市政交通一卡通系统安全的通用技术要求，包括卡片安全、终端安全、系统安全、交易安全、密钥管理及算法要求、国密算法应用标准。

本文件适用于市政交通一卡通系统安全的设计、开发、实施、验收、运营与管理。

1. 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，仅所注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 18238.3 信息技术 安全技术 散列函数 第3部分：专用散列函数

GB/T 22239 信息安全 网络安全等级保护基本要求

GB 50174 数据中心设计规范

GM/T 0002 SM4分组密码算法

GM/T 0003 SM2椭圆曲线公钥密码算法

GM/T 0004 SM3密码杂凑算法

JR/T 0025 中国金融集成电路（IC）卡规范

JT/T 978.2 城市公共交通IC卡技术规范第2部分：卡片

JT/T 978.6 城市公共交通IC卡技术规范第6部分：安全

JT/T 1059.5 交通一卡通移动支付技术规范 第5部分:客户端软件

JT/T 1059.6 交通一卡通移动支付技术规范 第6部分:可信服务管理系统

DB11/T 159.1 市政交通一卡通技术规范 第1部分：总则

DB11/T 159.2 市政交通一卡通技术规范 第2部分：卡片

DB11/T 159.3 市政交通一卡通技术规范 第3部分：终端

ISO/IEC 9798 信息技术-安全技术-实体鉴别

ISO/IEC 10116 信息技术 安全技术n位块密码算法的操作方式

ISO 16609 金融服务 采用对称加密技术进行报文鉴别的要求

1. 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

* 1.

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。

* 1.

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，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。

* 1.

移动支付 mobile payment

通过移动支付终端进行账务支付的一种方式。

[来源：JT/T 1059.1—2016,3.2，有修改]

* 1.

电子钱包 electronic purse(EP)

一种为小额消费而设计的IC卡应用，支持充值、消费等交易。

* 1.

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。

* 1.

明文 plaintext

没有加密的信息。

* 1.

密文 ciphertext

通过密码系统产生的不可理解的文字或信号。

* 1.

密钥 key

对数据进行加密时使用的秘密参数，可利用密钥对密文解密，使原数据文件恢复。

* 1.

终端设备 terminal

能完成一卡通卡应用的IC卡读写设备，从物理配置上分为A、B两类终端，两类终端都可以用来实现充值、消费或服务功能。

* 1.

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。

* 1.

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。

* 1.

Timing攻击 Timing attack

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，利用这些漏洞进行的攻击活动。

* 1.

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，来提取与密钥有关信息的攻击活动。

* 1.

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。

* 1.

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。

* 1.

认证 authentication

确认一个实体所宣称的身份的措施。

[来源：JT/T 978.6—2015,3.7]

* 1.

证书 certificate

由密钥管理系统使用其私钥对实体的公钥、身份信息以及其他相关信息进行签名，形成的不可伪造的电子数据。

[来源：JT/T 978.6—2015,3.8]

* 1.

安全域 security domain

负责对某个SE外实体（例如SE发行方、应用提供方、授权管理者）的管理、安全、通信需求进行支持的SE内实体。

[来源：JT/T 1059.1—2016,3.14]

* 1.

可信服务管理 trusted service management （TSM）

由可信第三方提供的安全载体生命周期管理、应用生命周期管理和应用管理等服务。

[来源：JT/T 1059.1—2016,3.18]

* 1.

客户端 client

用于提供用户接口界面，与SE配合实现SE管理及应用管理功能的应用软件。

[来源：JT/T 1059.6—2016,3.1]

1. 缩略语

DB 11/T 159.1界定的以及下列缩略语适用于本文件

ADF：应用定义文件（Application Definition File）

AEF：应用基本文件（Application Elementary File）

CA：证书认证中心（Certificate Authority）

CPU：中央处理单元（Central Process Unit）

DES：数据加密标准（Data Encryption Standard）

EF：基本文件(Elementary File）

FCI：文件控制信息（File Control Information）

FCP：文件控制参数（File Control Parameter）

IC：集成电路（Integrated Circuit）

MAC：报文验证码（Message Authorization Code）

PIN：个人识别码（Personal Identification Number）

PKI：公开密钥基础设施（Public Key Infrastructure）

RSA：一种非对称加密算法（Rivest,Shamir,Adleman）

SAM：安全认证模块（Secure Authentication Module）

SHA：安全哈希算法（Secure Hash Algorithm）

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）

SN：序号（Serial Number）

TSM：可信服务管理（Trusted Service Management）

1. 卡片安全
	1. 一般性要求

应符合JT/T 978.6相关要求。

* 1. 共存应用

不同应用之间应设计“防火墙”以防止跨过应用进行非法访问。包括所有不在本规范中定义中的其他应用。

不同应用之间的初始化要求和应用规则不应发生冲突。

* 1. 密钥的独立性

特定功能的加密/解密密钥不能被任何其他功能所使用，包括保存在卡片中的密钥和用来产生、派生、传输这些密钥的密钥。

* 1. 卡片内部安全体系
		1. 卡片内部安全目标

为了保证卡片操作系统使用合适的安全机制，并在卡片内部为所有数据及处理过程提供安全性和完整性保障，实现卡片命令加解密及鉴权，和卡内数据文件的安全访问控制。

* + 1. 卡片内部安全概述
			1. 一般要求

安全体系的基础结构包括两个基本特性：

1. “安全域”的建立
2. 对每个EF的存取采用指定的访问条件。
	* + 1. 安全域

卡片内部安全域应满足如下要求：

1. 操作系统控制对所有数据和可执行资源（即数据文件、记录、命令和加密密钥与算法）的访问，应通过执行选择（SELECT）和获取处理选项（GPO）命令实现安全域。这些命令建立描述安全域的相关信息，并定义数据和可执行资源的范围；
2. 由于卡片操作系统是在文件层次上使用这些信息和实现对数据的访问控制，发卡机构不应将同一层次下访问条件不同的数据并到同一个文件中；
3. 应使用选择（SELECT）命令访问应用管理数据（AMD），AMD指定能够被后续指令访问的所有数据文件，记录以及可执行资源；
4. 应用管理数据决定可访问的文件和可执行资源，文件和记录编号应在获取处理选项（GPO）命令响应内的应用文件定位器（AFL）中提供；
5. 发卡机构应限制在交易期间被存取的资源，应用管理数据的初始化状态（在个人化阶段被定义）应仅包含交易过程中可被访问的数据文件；
6. 初始的应用管理数据应在选择应用时建立，并且在个人化时被定义。
	* + 1. 基本文件（EF）访问条件

对于基本文件的访问，前提是至少执行一次选择（SELECT）命令并且安全域已经建立。一旦安全域建立，并且后续读取（如读记录命令）或者更新数据（如修改记录命令）命令被发送到一个基本文件的时候，基本文件的访问控制（由文件控制信息的文件控制参数定义）被强制使用。使用安全通信或VERIFY命令（或者包含二者）作为访问条件的文件只有在这些条件都满足以后被请求的访问才能继续执行。基本文件的访问条件应用于所有命令，以提供对卡片数据的外部访问，如读记录（READ RECORD）、取数据（GET DATA）、设置数据（PUT DATA）、修改记录（UPDATE RECORD）等命令。

* + 1. 文件控制信息
			1. 概述

文件控制信息（FCI）描述了文件的特性，附属于每个ADF或AEF。文件控制信息在个人化时建立，定义了初始的安全域。

* + - 1. 应用管理数据
				1. 安全域的定义

应用管理数据描述的安全域定义以下内容：

1. 在应用范围内可以被存取的资源，应用基本文件和内部基本文件（如个人识别码PIN、密钥、参数）；
2. 可在应用的上下文范围内被执行的命令；
3. 命令与资源之间的关系。
	* + - 1. 安全域定义的资源类型

安全域由应用管理数据说明的相关资源定义。没有被包含在应用管理数据内的资源不能被应用所使用。对应用来说安全域是相互独立的。共有以下两类资源被定义：数据资源、可执行代码资源。

* + - 1. 数据资源
				1. 一般要求

数据资源可以是数据文件及其记录、密钥、PIN的任意一个。

* + - * 1. 数据标识

数据资源是指文件内的数据元，由卡片内部的唯一标识符识别。文件由卡片内部唯一的文件标识符标识。不包含在文件内的数据元则由一个唯一数据标识标识。运行应用所需的任何数据资源应在应用管理数据内标识，要求如下：

1. 对包含了数据元（可由应用管理数据定义的命令访问）的文件而言，SFI（在应用内被唯一标识，并且可从外部被引用）与文件标识（在卡片内被唯一标识，并且可从内部被引用）之间的关系被维护在应用管理数据内。
2. 对未被包含在文件内的数据对象[可由应用管理数据定义的命令如取数据（GET DATA）命令访问]而言，数据对象标签（可从外部被引用）与唯一数据标识（在卡片内部，并且可从内部被引用）之间的关系被维护在应用管理数据内。
	* + - 1. 密钥标识

密钥不应从外部被引用。对保存在文件内的密钥，应用管理数据维护了在执行应用管理数据定义的命令和加密算法时定位密钥所必需的文件标识和指向密钥的引用；对不保存在文件内的密钥，应用管理数据维护了在执行应用管理数据定义的命令和加密算法时定位密钥所必需的卡片内部的唯一密钥标识。

* + - * 1. 可执行代码资源

可执行代码资源包括：命令、加密算法。

* + - * 1. 命令标识

命令资源包括CLA和INS字节，操作系统用他们来查找命令的位置。命令资源项包括了命令访问的数据的属性，有时还有与密钥和算法相关的参数属性。

* + - * 1. 算法标识

算法标识是为应用而定义的，与操作系统用来定位可执行代码的实际算法引用之间的联系。算法标识定义了卡片操作系统中卡片操作指令所使用的密码算法类型。

* + 1. 文件控制参数

每个基本文件的文件控制信息中都包含一个文件控制参数（FCP），文件控制参数保存了文件的访问条件控制信息。该信息在卡片个人化期间写入卡片内，与卡片应用管理数据一起，构建了卡片数据文件访问控制的安全体系。基本文件的访问见表1。

1. 基本文件的访问条件

|  |  |  |
| --- | --- | --- |
| 读取 | 更新 | 访问条件 |
| 是/否 | 是/否 |  |
| 是/否 | 是/否 | 安全通信 |
| 是/否 | 是/否 | 校验 |
| （不可用） | 是/否 | 数据加密 |
| 注1：读取一栏表示使用读取命令，如读记录（READ RECORD）或取数据（GET DATA）命令，存取基本文件内部的数据。“更新”一栏表示使用更新命令，如修改记录（UPDATE RECORD）或设置数据（PUT DATA）命令，存取基本文件内部的数据。注2：文件控制参数指出是否在发卡机构脚本修改记录（UPDATE RECORD）命令中以加密或者明文格式传送数据。注3：文件控制参数也作为一个组件用于实现应用管理数据的逻辑结构。 |

* + 1. 卡片本地数据的访问条件

数据访问条件适用于可被读记录（READ RECORD）、修改记录（UPDATE RECORD）、取数据（GET DATA）命令或其他合适的类似命令访问的数据.

* 1. 卡片通信安全

卡片通信安全应满足要求如下：

1. 一卡通卡应采用一卡一密的密钥管理体系，卡的密钥利用卡的序列号（SN）及其他有关信息，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，记录在一卡通卡中；
2. 卡片应用验证应通过内置在终端的SAM卡或安全模块，与总中心计算机处理系统金融加密机完成；
3. 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/IEC 9798规定方法鉴别；
4. 卡片在每次写操作时，均应经过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，MAC的具体算法应符合附录A、附录B的要求
	1. 卡片交易安全

卡片交易安全应满足要求如下：

1. 卡片消费交易流程安全应满足交通部行业应用规范，电子钱包应用应完全符合 JT/T978.2中的消费交易要求；
2. 卡片充值交易流程安全应满足交通部行业应用规范，电子钱包应用应完全符合 JT/T978.2中的充值交易要求。
	1. 卡片防攻击
		1. 防Timing攻击

应能够抵御通过卡片CPU运算的时间差异分析卡片机密信息的攻击。

* + 1. 防SPA/DPA攻击

应能够抵御卡片计算过程中能量消耗的变化而泄露卡片机密信息的攻击。

* + 1. 防随机数攻击

卡片随机数的产生应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。

* 1. 卡片国密算法要求

卡片芯片及操作系统需支持国密SM2、SM3、SM4算法。

1. 终端安全
	1. 终端数据安全

终端存在两种基本类型的数据，包括：

1. 业务数据：如终端交易记录等。外界可以对这些数据进行访问，但不允许进行无授权修改；
2. 密钥数据：包括卡片应用密钥、公私钥、及终端内部参数。在未授权的情况下，外界不允许对这类数据进行访问和修改。
	* 1. 通用数据的安全要求

通用数据应存放在存储器中。在更新参数以及下载新的应用程序时，终端应执行以下操作：

1. 验证更新方的身份；
2. 校验下载参数及应用程序的完整性；
3. 在任何情况下，终端的应用数据都不会随意改变或丢失，并保证数据有效；
4. 所有与交易相关的数据均应以记录形式存储于终端存储器中，终端须保证这些数据的完整性。
	* 1. 密钥数据的安全要求

敏感数据应存放在终端安全模块SAM中。安全模块应保证存储数据的安全，具体要求如下：

1. 安全模块提供必要的安全机制以防止外界对终端所储存或处理的数据进行非法攻击的硬件加密模块。这些数据包括各种密钥和内部参数；
2. 安全模块的硬件设计应能保证在物理上限制对其内部存贮的敏感数据的存取，以及对安全模块的非授权使用和修改。一旦安全模块受到非法的攻击，其自身应能够立即完成对内部敏感数据的删除；
3. 安全模块的逻辑设计应保证，调用任何单一功能或组合功能，都不会导致敏感数据的泄露。对于某些敏感操作，应有一定的权限限制。
	1. 终端设备安全
		1. 基本要求

设备应具有防入侵功能，保证在正常的运行环境中，设备及其接口不会泄露、改变任何输入/输出设备的、存储在设备中的、在设备中处理的敏感数据。

* + 1. 一般要求

终端应限制对内部存储的密钥数据、业务参数、个人敏感信息的物理访问，并且阻止窃取数据，未经授权的使用或者未经授权的对设备的修改应有安全控制，具体要求如下：

1. 不应允许入侵设备并对设备的软硬件进行增加、替换或修改；
2. 不应允许测定或修改任何敏感数据后重新安装设备；
3. 当设备的任何部件发生故障时，不会导致秘密或敏感数据的泄露；
4. 如果设备的设计需要部分部件在物理上分离，并且处理的数据或指令在这些分离的部件之间传递，那么对设备的所有部件的保护等级应是相同的。
	1. 终端密码算法要求
5. 终端硬件需支持的国际算法：3DES、RSA、SHA等；
6. 终端硬件需支持的国密算法：SM2、SM3、SM4；
7. 终端需满足各类对称、非对称密钥，国际、国密密钥的安全下发、存储和更新。
8. 系统安全
	1. 通用要求

系统安全不低于 GB/T 22239中第三级的要求；

* 1. 安全物理环境
	2. ·安全通信网络
		1. 网络架构
1. 应保证网络设备的业务处理能力满足业务高峰期需要；
2. 应保证网络各个部分的带宽满足业务高峰期需要；
3. 应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；
4. 应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段；
5. 应提供通信线路、关键网络设备的硬件冗余，保证系统的可用性。
	* 1. 通信传输
6. 应采用校验技术或密码技术保证通信过程中数据的完整性；
7. 应采用密码技术保证通信过程中敏感数据的保密性。
	1. 安全区域边界
		1. 边界防护
8. 应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信；
9. 应能够对非授权设备私自联到内部网络的行为进行检查或限制；
10. 应能够对内部用户非授权联到外部网络的行为进行检查或限制；
11. 应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。
	* 1. 访问控制
12. 应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；
13. 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；
14. 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；
15. 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力；
16. 应对进出网络的数据流实现基于应用协议和应用内容的访问控制。
	* 1. 入侵防范
17. 应在关键网络节点处检测、防止或限制从内、外部发起的网络攻击行为；
18. 应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析；
19. 当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。
	* 1. 恶意代码防范

应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。

* 1. 安全计算环境
		1. 身份鉴别
1. 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；
2. 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；
3. 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；
4. 应采用两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用动态口令、密码技术或生物技术来实现。
	* 1. 访问控制
5. 应对登录的用户分配账户和权限；
6. 应重命名或删除默认账户，修改默认账户的默认口令；
7. 应及时删除或停用多余的、过期的账户，避免共享账户的存在；
8. 应进行角色划分，并授予管理用户所需的最小权限，实现管理用户的权限分离；
9. 应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；
10. 访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；
11. 应对敏感信息资源设置安全标记，并控制主体对有安全标记信息资源的访问。
	* 1. 数据完整性
12. 应采用校验码技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据等；；
13. 应采用校验码技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据等。
14. 数据保密性；
15. 应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据等；
16. 应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据等。
	* 1. 数据恢复和备份
17. 应提供重要数据的本地数据备份与恢复功能；
18. 应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；
19. 应提供重要数据处理系统的热冗余，保证系统的高可用性。
	* 1. 剩余信息保护
20. 应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除；
21. 应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。
	1. 安全管理中心
		1. 系统管理
22. 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；
23. 应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。
	* 1. 审计管理
24. 应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；
25. 应通过审计管理员对审计记录应进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。
	* 1. 安全管理
26. 应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计；
27. 应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。
	* 1. 集中管控
28. 应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控；；
29. 应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理；
30. 应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测；
31. 应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求；
32. 应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；
33. 应能对网络中发生的各类安全事件进行识别、报警和分析。
	1. 云计算扩展要求
34. 应确保云计算基础设施位于中国境内；
35. 应保证云计算平台不承载高于其安全保护等级的业务应用系统；
36. 应实现云内虚拟网络之间的隔离；
37. 应具有通信传输、边界防护、入侵防范等安全机制的能力；
38. 应具有自主设置安全策略的能力，包括定义访问路径、选择安全组件、配置安全策略；
39. 应在虚拟化网络边界部署访问控制机制，并设置访问控制规则；
40. 应建立双向身份验证机制；
	1. 移动互联扩展要求
41. 应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备；
42. 无线接入设备应开启接入认证功能，并支持采用认证服务器认证或国家密码管理机构批准的密码模块进行认证；
43. 应能够检测、定位和阻断到非授权无线接入设备或非授权移动终端；
44. 应能够检测到针对无线接入设备的网络扫描、DDOS攻击、密钥破解、中间人攻击和欺骗攻击等行为；
	1. 移动支付系统安全要求
		1. 可信服务管理系统安全要求

移动支付系统可信服务管理系统的安全要求应符合JT/T 1059.6中的6.3平台安全要求。

* + 1. 客户端软件安全要求

客户端软件的安全要求应符合JT/T 1059.5中的7、安全技术要求。

1. 交易安全
	1. 消费类交易安全

消费类交易处理应保证卡与终端之间、终端与系统之间的数据正确传输，防止数据被非法窃取或篡改，具体要求如下：

1. 公共交通领域消费终端应使用SAM完成卡片的脱机交易验证；
2. 非公共交通领域消费终端应使用完成卡片的脱机交易验证；消费交易所需安全性较高的行业及应用，应采用联机消费方式进行；
3. 消费交易时，应先验证卡的合法性，如是否为本系统卡、卡片状态是否正常等；
4. 消费交易时，应验证卡的可用性，如是否为黑名单卡、是否为可用卡、余额是否足够等；
5. 消费交易应符合中心计算机系统下发的消费类参数规定，如消费可用卡类型等；
6. 消费成功后应正确生成和完整保存消费交易数据，并确保数据存储的安全性；
7. 消费交易数据应包含TAC；
8. 系统应及时将黑名单下发到每一台终端上，终端应拒绝黑名单卡的交易并进行锁卡。
	1. 充值类交易安全

充值类交易处理应保证卡与终端之间、终端与系统之间的数据正确传输，防止数据被非法窃取或篡改，具体要求如下：

1. 充值类交易应采用联机方式进行，即交易过程中，终端与总中心计算机处理系统实时通信，通过终端及其内置的安全模块、认证系统及硬件加密机，完成卡片的联机认证及合法性检查；
2. 联机交易终端与总中心计算机处理系统的交互流程应采用PKI体系安全机制，采用非对称算法及动态工作密钥报文加密技术，确保传输报文的安全，报文中附带MAC校验码防篡改；
3. 支持充值类业务的终端应成功签到取得授权，并在有效时间范围内进行一卡通卡的充值类交易，授权验证的权限应在断电、复位、关机或超时后失效；
4. 总中心计算机处理系统应具有对支持充值类业务的终端、商户、单位充值额度的三级配置管理功能，如：累计充值额度、当日最大充值额度限制等，对超出充值额度的终端、商户和单位，系统应拒绝其继续交易；
5. 充值交易时，应验证卡的合法性和可用性，包括是否为本系统卡、卡片状态是否正常、是否为黑名单卡等；
6. 充值成功后，终端应正确生成和完整保存充值交易数据，并将交易数据实时上传至总中心计算机处理系统；
7. 充值交易数据应包含TAC。
	1. 退卡类交易安全

退卡类交易处理应保证卡与终端之间、终端与系统之间的数据正确传输，防止数据被非法窃取或篡改，具体要求如下：

1. 退卡类交易应采用联机方式进行，即交易过程中，终端与总中心计算机处理系统实时通信，通过终端及其内置的安全模块、总中心计算机处理系统及硬件加密机，完成卡片的联机认证及合法性检查；
2. 联机交易终端与总中心计算机处理系统的交互流程应采用PKI体系安全机制，采用非对称算法及动态工作密钥报文加密技术确保传输报文的安全，报文中附带MAC校验码防篡改；
3. 退卡类终端应成功签到取得授权，并在权限有效时间范围内进行一卡通卡的退卡退资交易，授权验证的权限应在断电、复位、关机或超时后失效；
4. 退卡类交易应符合总中心计算机处理系统下发的退卡类参数规定；
5. 退卡交易时，应先验证卡的合法性和可用性，包括是否为好卡、是否为本系统卡、卡片状态是否正常、是否为黑名单卡等；
6. 卡片合法性、可用性、参数符合性验证，由终端和总中心计算机处理系统共同完成，通过验证的卡准许进行交易；
7. 退卡退资成功后，终端应正确生成和完整保存交易数据，并将交易数据实时上传至总中心计算机处理系统；
8. 退卡退资交易数据应包含TAC。
9. 密钥管理及算法
	1. 通用要求

市政交通一卡通系统密钥管理应符合JT/T 978 行业标准的规定。

* 1. 生成与发行
		1. 密钥生成
			1. 生成方式

生成方式要求如下：

1. 对称密钥应采用集中方式生成，即由管理机构生成相应的主密钥组，其他密钥由该组主密钥分散生成。密钥生成的两种基本方法为：
2. 不重复的密钥生成：随机生成不可恢复的密钥，每次的数值不相同；
3. 可重复的密钥生成：密钥变换、密钥衍生；密钥的生成是可重复的，在需要的情况下，能够重新得到与原来相同的密钥值。
4. 非对称密钥应采用在加密机或SAM卡内部产生公私钥密钥对，私钥在加密机或SAM卡内存储，公钥输出外部的方式产生；
5. 数字证书应采用根CA逐级向下签发的方式产生用户证书或设备证书。
	* + 1. 安全技术

不需重复生成的密钥应采用随机产生的方式生成，由系统随机产生密钥，写入安全存取模块中保存；可重复生成的密钥采用密钥变换或密钥衍生的方式生成，应确保密钥变换或密钥衍生过程绝对安全。

* + - 1. 安全措施

为了保证密钥的安全，防止密钥的泄露，在密钥生成时，应采取以下措施：

1. 密钥生成采用多人生成或硬件加密的方式；
2. 密钥生成应有独立的物理空间，环境应符合安全管理要求；
3. 密钥生成应由专人负责，应符合安全管理规定；
4. 密钥生成的过程应按照严格的操作规程进行。
	* 1. 密钥发行
			1. 发行方式

密钥发行应采用梯级生成、下发方式。即由上一级生成下一级所需的各种子密钥，并以卡片的形式传递给下一级。

* + - 1. 安全技术

应使用传输密钥控制密钥的加密装载、直接加密导出、分散加密导出。

* 1. 安全机制
		1. 对称加密技术

对称加密技术，包括数据加解密、报文鉴别码算法、过程密钥的产生、子密钥分散，应符合JT/T 976.6中9.1、9.2相关要求。

* + 1. 非对称加密技术

非对称加密技术用来进行静态数据和动态数据的验证以及数字签名，应符合JT/T 976.6中9.3、9.4相关要求。

在选择公开密钥的模数长度时，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。

发卡方公开密钥的指数长度与IC卡公开密钥的指数长度由发卡方决定。

* 1. 密钥算法
		1. 对称加密算法

对称加密算法包括如下：

1. DES\3DES算法，算法按ISO 16609、ISO/IEC 10116执行；
2. SM4算法，算法按GM/T 0002执行。
	* 1. 非对称加密算法

非对称加密算法包括如下：

1. RSA算法，算法按JR/T 0025执行；
2. SM2算法，算法按GM/T 0003执行。
	* 1. 安全哈希算法

安全哈希算法包括如下：

1. SHA-256算法，算法按GB/T 18238.3执行；
2. SM3算法，算法按GM/T 0004执行。
	1. 国密算法对称加密机制
		1. 加密解密

对数据的加密采用 16 字节分组加密算法，根据交通部标准规范JT/T 978.2，需选用 ECB 模式作为加密解密模式。

用加密过程密钥 KS对任意长度的报文 MSG 加密的步骤如下：

* + - * 1. 填充并分块

如果报文 MSG 的长度不是分组长度的整数倍， 在 MSG 的右端加上 1 个‘80 字节，然后再在右端加上最少的‘ 00’字节，使得结果报文的长度 MSG： =(MSG||‘80’ ||‘ 00’ ||‘00’ ||....||‘00’ )是分组长度的整数倍。

如果报文 MSG 的长度是分组长度的整数倍，不对数据作填充。

被加密数据首先要被格式化为以下形式的数据块：

1. 明文数据的长度，不包括填充字符；
2. 明文数据；
3. 填充字符（按上述填充方式）。

然后 MSG 被拆分为 16 字节的块 X1， X2，..， Xk。

* + - * 1. 密文计算
	1. ECB 模式

用加密过程密钥 KS， 以 ECB 模式的分组加密算法将块 X1， X2， . . . , XK 加密为 16 字节的块 Y1, Y2, . . . , YK， 因此当 i ＝ 1, 2, „ , K 时分别计算： Yi := ALG(KS)[Xi]。

* 1. CBC 模式

用加密过程密钥 KS以 CBC 模式的分组加密算法将块 X1， X2， . . . , XK 加密为 16 字节的块 Y1, Y2, . . . , YK， 因此当 i ＝ 1, 2, „ , K 时分别计算： Yi := ALG(KS)[Xi⊕ Yi-1]

* + - * 1. 解密过程如下：

1) ECB 模式

当 i = 1, 2, ... , K 时， 分别计算： Xi := ALG-1(KS)[Yi ]。

2) CBC 模式

当 i = 1, 2, ... , K 时， 分别计算： Xi := ALG-1(KS)[Yi ]⊕ Yi-1。

为了得到原来的报文 MSG，将块 X1, X2, ... , XK连接起来，如果使用了填充，从最后一块 Xk中删除除尾部的(‘ 80’ || ‘ 00’ || ‘ 00’ || ... || ‘ 00’ )， 记为： MSG = DEC(KS)[Y]。

* 1. 国密算法非对称加密机制
		1. 算法

本文件使用GM/T 0003 的椭圆曲线算法进行数字签名算法和数字签名验证。

SM2签名方案使用下面三种函数：

1. 一个依赖于私钥 SK的签名函数 Sign(SK)[M]，该函数输出两个相同长度的数字 r 和 s；
2. 一个依赖于公钥 PK 的验证函数 Verify(PK)[M, Sign(SK)[M]]，该函数输出 True 或 False，表示验证正确或失败；
3. 一个哈希算法 SM3，将任意长度的报文映射为一个 32 字节的哈希值。
	* 1. 数字签名产生

对任意长度的数据组成的报文MSG计算签名S的过程如下：

1. 计算ZA=SM3[ENTLA || IDA || a || b || xG ||yG || xA || yA]。其中IDA固定设置为16字节定
2. 长的十六进制数据0x31, 0x32, 0x33, 0x34, 0x35, 0x36, 0x37, 0x38, 0x31, 0x32, 0x33,
3. 0x34, 0x35, 0x36, 0x37, 0x38； ENTLA值为两个字节数据0x00, 0x80；
4. 计算报文MSG的32字节的HASH值 h:= SM3 [ZA||MSG]；
5. 计算Sign(SK)[h]，得到两个数字r和s；
6. 数字签名S被定义为S:= r||s，即数字签名S由数字r和s串联而成。
	* 1. 数字签名验证

对任意长数据组成的报文MSG验证签名S的过程如下：

1. 计算ZA=SM3[ENTLA || IDA || a || b || xG ||yG || xA || yA]。其中IDA固定设置为16字节定
2. 长的十六进制数据0x31, 0x32, 0x33, 0x34, 0x35, 0x36, 0x37, 0x38, 0x31, 0x32, 0x33,
3. 0x34, 0x35, 0x36, 0x37, 0x38； ENTLA值为两个字节数据0x00, 0x80；
4. 计算报文MSG的32字节的HASH值 h:= SM3 [ZA||MSG]；
5. Verify(PK)[h, S]，若函数输出True表示验证正确，若输出False，表示验证失败。
6. （规范性）
MAC计算—DEA算法

按照如下的方式使用单重或三重DEA加密方式产生MAC：

第一步：取4个字节随机数，后补4字节的十六进制数字‘0’作为初始变量。

第二步：按照顺序将以下数据连接在一起形成数据块：

1. CLA，INS，P1，P2，Lc；
2. 所有在市政交通卡应用规范中定义的数据；
3. 在命令的数据域中（如果存在）包含明文或加密的数据（例：如果要更改个人密码，加密后的个人密码数据块放在命令数据域中传输）。

第三步：将该数据块分成8字节为单位的数据块，标号为D1，D2，D3，D4等。最后的数据块有可能是1-8个字节。

第四步：如果最后的数据块长度是8字节，则在其后加上十六进制数字‘80 00 00 00 00 00 00 00’，转到第五步。

如果最后的数据块长度不足8字节，则在其后加上十六进制数字‘80’，如果达到8字节长度，则转入第五步；否则在其后加入十六进制数字‘0’直到长度达到8字节。

第五步：对这些数据块使用卡片维护密钥进行计算 （MAC的产生如图A.1中所示），根据第二步产生的数据块的长度，计算过程有可能多于或少于四步。

第六步：最终取得的MAC值是从计算结果左侧截取的4字节数值。

下图为DEA加密方式产生MAC示意：



图A.1 双长度DEA Key的MAC算法

1. （规范性）
MAC计算—SM4算法

按照如下的方式使用SM4加密方式产生MAC：

第一步：取4字节/8字节随机数，后补12字节/8字节十六进制数‘00’作为初始值。

第二步：将所有输入数据按指定顺序连接成一个数据块。

第三步：将该数据块分成以分组长度16个字节为单位的数据块，表示为：块1、块2…块n。

第四步：在最后的数据块后加入十六进制数‘80’，如果此时达到分组长度，则转到第五步，否则在其后加入十六进制数‘00’，直到长度达到分组长度。

第五步：按图B.1所述的算法对这些数据块使用指定的密钥进行加密。

第六步：将16字节运算结果按4字节分块做异或运算得到报文认证码MAC。

下图为SM4加密方式产生MAC示意：

 

图B.1 SM4的MAC算法