附件

广东省全国交通一卡通
密钥管理技术规范

目录

编写说明

为规范我省全国交通一卡通互联互通工作，解决实施过程中密钥生成、使用和管理等相关问题，根据《城市公共交通 IC 卡技术规范》（JT/T 978-2015）等规定和标准，制定《广东省全国交通一卡通密钥管理技术规范》（以下简称《技术规范》）。

本《技术规范》在编写过程中，采纳了广东省内地级以上市交通运输主管部门及各地市交通一卡通运营机构提出的合理建议，借鉴了各系统集成商、设备供应商的成功经验。

术语定义

密钥

特指由阿拉伯数字“0-9”和英文字母“A-F”组成，存储于卡片或硬件设备中，用于保护敏感数据的字串。

密钥母卡

一张用于存储密钥数据的卡片。

加密

以某种特殊的策略机制将原有的信息内容改变成特定的数据，使得未授权的用户即使获得了数据，仍然无法了解信息内容的一种方法。

解密

以某种特殊的策略机制还原加密数据，使得授权的用户了解信息内容的一种方法。

加密机（Host Security Module）

由国家密码管理局鉴定并批准，具有安全硬件模块，用于密钥存储、数据加密和解密以及数据验证的服务器，英文缩写“HSM”。

地市机构

特指广东省内经由地级以上市交通运输主管部门委托的地市交通一卡通运营机构。

地市机构代码

由交通运输部统一分配给地市机构的数字识别码。

密钥分散

使用上一级密钥和本级特征，按特定算法进行计算，形成本级密钥的过程。

根密钥

人工或自动生成，用于后续密钥分散的原始密钥。

省级根密钥

一组由省级交通运输主管部门生成和管理的，用于开展广东省全国交通一卡

通统一充值、消费优惠和客服等业务的根密钥。

省级业务密钥

一组由省级根密钥分散，用于统一充值、消费优惠和客服等业务的密钥。

密钥管理系统

一套部署在服务器上，用于对多台加密机进行密钥管理的软件。

对称密钥

加密和解密过程都使用相同密钥的一种密钥数据。密钥须以安全的形式进行约定和传递。

非对称密钥对

加密和解密过程使用不同密钥的一种密钥数据，它由公开密钥（简称“公钥”）和私有密钥（简称“私钥”）组成，加密和解密过程中分别使用公钥与私钥。

加密机维保

对加密机中的密钥数据进行配置和管理，使其保持正常状态的一组操作。

加密机维保密钥对

一组用于加密机维保的非对称密钥对。

加密机维保客户端

一套通过网络端口与加密机进行连接，用于加密机维保的软件。

密钥分量

特指由阿拉伯数字“0-9”和英文字母“A-F”组成，存储于保密信封，用于合成密钥的字串。

口令

特指由阿拉伯数字“0-9”组成，由操作人员设定并保管，用于身份验证的数字串。

加密机管理员角色

具有特定加密机管理权限的人物身份。

加密机管理员

被赋予加密机管理员角色的个人，可对加密机进行参数配置、密钥导入导出和设备管理。

加密机管理员卡

一张配发给加密机管理员，用于加密机对管理员进行身份识别的卡片。

加密机管理员口令

一组由加密机管理员设定并存储于加密机中，用于对管理员进行身份识别的口令。

加密机设备密钥

一条用于保护加密机中密钥数据的密钥。

加密机设备密钥分量

一组用于加密机设备密钥合成的密钥分量。

加密机设备密钥分量口令

一组用于替代加密机设备管理员卡进行身份识别的口令。

加密机传输密钥

一条用于保护密钥传输或交互的密钥。

加密机传输密钥分量

一组用于加密机传输密钥合成的密钥分量。

加密机管理软件

一套通过网络端口与加密机进行连接，用于管理单台加密机的软件。

明文

信息内容未被加密的数据。

密文

信息内容经过加密的数据。

指令

特指让设备执行某一特定操作的代码。

算法

加密和解密过程中使用的一种策略机制。

白名单

一组具有合法许可权限的名单数据。

椭圆曲线公钥密码算法

国家密码管理局发布的椭圆曲线非对称密码算法，简称“SM2”。

分组对称密钥算法

国家密码管理局发布的分组密码对称加密算法，简称“SM4”。

数据加密标准（Data Encryption Standard）

国标化标准组织发布的一种对称数据加密标准，英文缩写“DES”。

RSA 算法（Rivest－Shamir－Adleman algorithm）

国标化标准组织发布的一种非对称密钥对算法，由罗纳德·李维斯特（Ron Rivest）、阿迪·萨莫尔（Adi Shamir）和伦纳德·阿德曼（Leonard Adleman）提出，英文缩写“RSA”。

公钥基础设施（Public Key Infrastructure）

一种利用非对称密钥对技术为基础的安全体系，英文缩写“PKI”。

专用安全存取模块（Purchase Secure Access Module）

一种用于储存消费业务根密钥的安全存取设备，英文缩写“PSAM”。

报文鉴别码（Message Authentication Code）

一种对信息按照特定算法进行计算得到的信息数据，英文缩写“MAC”。

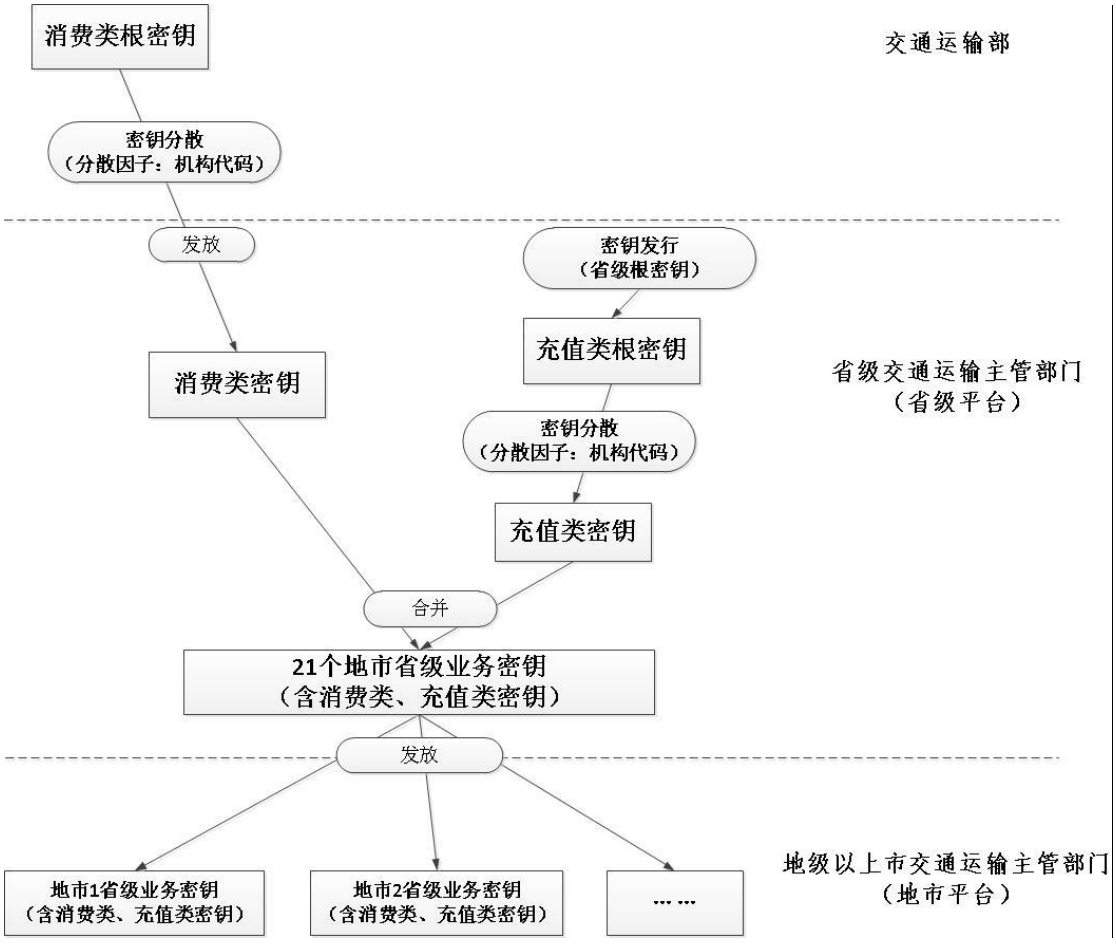
第一章 密钥管理技术规范

第一节 密钥体系

1. 体系说明

本《技术规范》中的一卡通密钥按功能分为两类，一类是消费类密钥，另一类是充值类密钥。

省级交通运输主管部门负责发行省内统一的充值类密钥和向交通运输部申领消费类密钥，发放给各地级以上市交通运输主管部门使用并实施监管，如下图所示：



*注：机构代码详见《附录 1：广东省全国交通一卡通入网发卡机构信息》

2. 省级平台

省级平台由省级交通运输主管部门指导建设，省级交通一卡通运营机构负责运营，用于对接交通运输部全国交通一卡通数据交换中心和地市交通一卡通运营机构，具有密钥管理、集中票卡发行、PSAM/PKI 发行、统一充值、统一清分结算等功能。省级平台配置四种类型加密机：省级根密钥加密机、省级业务密钥加密机、省级清算密钥加密机和备用加密机。

3. 地市平台

地市平台由地级以上市交通运输主管部门或委托交通一卡通运营机构按照实际情况建设，用于对接省级平台，具有密钥管理、票卡发行、地市交易数据收集和地市结算等功能。地市平台配置两种类型加密机：地市业务密钥加密机和备用加密机。

4. 密钥载体

广东省全国交通一卡通密钥以省级交通运输主管部门指定的加密机和专用安全存取模块为载体。

加密机保存所有省级密钥，是实现密钥生成、导入、备份、发放的唯一设备，存放在专用机房，仅提供给特定的系统和用户使用。加密机必须符合《01GC_TEH_003-交通运输部城市公共交通卡系统加密机通用接口指令》（v2.3.1版本）以及《广东省全国交通一卡通加密机管理定制规范》（v1.5版本）。

专用安全存取模块仅存储消费业务根密钥，安装在交易终端上，用于交易鉴权和认证。专用安全存取模块的使用和保管严格按《城市公共交通 IC 卡技术规范》(JT/T 978-2015)执行。

4.1 密钥载体类型

根据所装载密钥的用途和提供的服务对密钥载体进行如下分类：

4.1.1 省级根密钥加密机

省级根密钥加密机是省级平台中存储与管理广东省全国交通一卡通省级根

密钥、加密机维保密钥对的加密机。

4.1.2 省级业务密钥加密机

省级业务密钥加密机是省级平台中存储对应地市广东省全国交通一卡通业务密钥的加密机，提供票卡发行、充值、在线交易所需的密钥服务。

4.1.3 省级清算密钥加密机

省级清算密钥加密机是省级平台中存储全省所有地市广东省全国交通一卡通清算密钥的加密机，为全省统一的清算业务提供交易验证服务。

4.1.4 地市业务密钥加密机

地市业务密钥加密机是地市平台中存储本地市广东省全国交通一卡通业务密钥的加密机，为地市交通一卡通运营机构自建的业务系统提供所需的密钥服务。

4.1.5 专用安全存取模块

专用安全存取模块是保存消费业务根密钥，安装在交易终端上，用于交易鉴权和认证。

第二节 密钥管理

1. 密钥管理员

密钥管理员是负责管理密钥载体和系统的相关人员，其权限设置及岗位分配应严格遵守本《技术规范》。

1.1 密钥管理员角色

密钥管理员主要有密钥监督员、加密机管理员和省级平台密钥管理系统管理员等角色。

1.1.1 密钥监督员

密钥监督员负责监督密钥安全管理的各项工作，即在整个密钥生命期内监督所有操作的合法性和规范性，制止不正确操作，杜绝违规操作或超越权限操作的行为。

1.1.2 加密机管理员

本《技术规范》定义以下四种加密机管理员角色：

设备管理员

设备管理员由 3 名加密机管理员组成，分别持有 1 张加密机管理员卡（以下分别称为“A1 卡”、“A2 卡”、“A3 卡”）。主要负责管理加密机其他管理员和设备密钥；

系统管理员

系统管理员由 1 名加密机管理员担任，持有 1 张加密机管理员卡（以下称为“B 卡”）。主要负责加密机网络通信端口的管理和维护工作；

安全管理员

安全管理员由 1 名加密机管理员担任，持有 1 张加密机管理员卡（以下称为“C 卡”）。主要负责加密机密钥数据的管理和维护工作；

审计管理员

审计管理员由 1 名加密机管理员担任，持有 1 张加密机管理员卡（以下称为“D 卡”）。主要负责加密机使用情况的审计工作。

1.1.3 省级平台密钥管理系统管理员

省级平台密钥管理系统定义两种管理角色，分别是系统配置员和系统密钥管理员。

系统配置员

系统配置员负责管理地市交通一卡通运营机构的基础信息、加密机部署信息及密钥管理员信息。

系统密钥管理员

系统密钥管理员负责广东省全国交通一卡通密钥的发放和管理工作。

为保障安全，省级平台密钥管理系统管理员角色的操作均要求双人执行，其中一人修改，另一人审核。

1.2 密钥管理员角色分配

1.2.1 密钥监督员角色分配

密钥监督员角色由省级交通运输主管部门指定。

1.2.2 省级根密钥加密机角色分配

设备管理员（A1 卡、A2 卡、A3 卡）

由 3 名省级交通运输主管部门或者省级交通一卡通运营机构密钥管理员共同组成，独立掌管加密机设备密钥分量、加密机设备密钥分量口令、加密机设备管理员的管理员卡及管理员口令。

系统管理员（B 卡）

由 1 名省级交通一卡通运营机构密钥管理员担任，掌管系统管理员的管理员卡及管理员口令。

安全管理员（C 卡）

由 1 名省级交通一卡通运营机构密钥管理员担任，掌管安全管理员的管理员卡及管理员口令。

审计管理员（D 卡）

由 1 名省级交通一卡通运营机构密钥管理员担任，掌管审计管理员的管理员卡及管理员口令。

1.2.3 省级业务密钥加密机角色分配

设备管理员（A1 卡、A2 卡、A3 卡）

由 3 名省级交通一卡通运营机构密钥管理员组成，独立掌管设备密钥分量、设备密钥分量口令、设备管理员的管理员卡及管理员口令。

系统管理员（B 卡）

由 1 名省级交通一卡通运营机构密钥管理员担任，掌管系统管理员的管理员卡及管理员口令。

安全管理员（C 卡）

由 1 名省级交通一卡通运营机构密钥管理员担任，掌管安全管理员的管理员

卡及管理员口令。

审计管理员（D 卡）

由 1 名省级交通一卡通运营机构密钥管理员担任，掌管审计管理员的管理员卡及管理员口令。

1.2.4 省级清算密钥加密机角色分配

设备管理员（A1 卡、A2 卡、A3 卡）

由 3 名省级交通一卡通运营机构密钥管理员组成，独立掌管设备密钥分量、设备密钥分量口令、设备管理员的管理员卡及管理员口令。

系统管理员（B 卡）

由 1 名省级交通一卡通运营机构密钥管理员担任，掌管系统管理员的管理员卡及管理员口令。

安全管理员（C 卡）

由 1 名省级交通一卡通运营机构密钥管理员担任，掌管安全管理员的管理员卡及管理员口令。

审计管理员（D 卡）

由 1 名省级交通一卡通运营机构密钥管理员担任，掌管审计管理员的管理员卡及管理员口令。

1.2.5 地市业务密钥加密机角色分配

设备管理员（A1 卡、A2 卡、A3 卡）

由 3 名省级或地级以上市交通运输主管部门密钥管理员组成，独立掌管设备管理员的管理员卡及管理员口令。

系统管理员（B 卡）

由 1 名地级以上市交通运输主管部门密钥管理员担任，掌管系统管理员的管理员卡及管理员口令。

安全管理员（C 卡）

由 1 名省级或地级以上市交通运输主管部门密钥管理员担任，掌管安全管理员的管理员卡及管理员口令。

审计管理员（D 卡）

由 1 名省级或地级以上市交通运输主管部门密钥管理员担任，掌管审计管理员的管理员卡及管理员口令。

1.2.6 省级平台密钥管理系统管理员角色分配

系统配置员（A 员、B 员）

由 2 名省级或地级以上市交通运输主管部门密钥管理员组成。

系统密钥管理员（A 员、B 员）

由 2 名省级或地级以上市交通运输主管部门密钥管理员组成。

2. 密钥生成

密钥必须随机或伪随机产生，其中随机指无法预知和重复，伪随机指由算法产生。密钥生成后，在密钥载体外部的明文形式必须由三个或以上的密钥分量构成。

2.1 省级根密钥

省级根密钥统一由省级交通运输主管部门采用加密机随机方式生成。

2.2 省级业务密钥

省级业务密钥统一由省级交通运输主管部门通过指定的密钥分散算法，从对应的省级根密钥分散得到。

2.3 加密机设备密钥

由密钥监督员逐个召集加密机设备管理员到指定的地点，按随机方法分别生成三个密钥分量并通过指定工具导入加密机中生成密钥。

每个加密机设备管理员生成并记录由其生成的密钥分量后，将该密钥分量装入专用的信封内封装并妥善保管。加密机设备管理员在生成和导入密钥期间，任何人员不得进入操作现场。

2.4 加密机传输密钥

由密钥监督员逐个召集传输密钥管理员到指定的地点，按随机方法分别生成

三个密钥分量并通过指定工具导入加密机中生成密钥。

每个传输密钥管理员生成并记录由其生成的密钥分量后，将该密钥分量装入专用的信封内封装并妥善保管。传输密钥管理员在生成和导入密钥期间，任何人员不得进入操作现场。

2.5 工作表格

在生成密钥的过程中，由操作人员按规定填写密钥生成表格，签名封存，表格作为密钥档案资料妥善保管，留底备查。

3. 密钥保管

3.1 密钥数据

对于广东省全国交通一卡通密钥的保管坚持三个原则，即最小化、认可化和高安全性。

最小化：广东省全国交通一卡通密钥载体内仅能存储省级交通运输主管部门指定的广东省全国交通一卡通密钥数据；

认可化：广东省全国交通一卡通密钥必须存放于省级交通运输主管部门指定的载体内，只有指定的密钥管理员可以进行操作；

高安全性：广东省全国交通一卡通密钥存放在指定的安全载体内，采用多重控制，不同角色的密钥管理员只拥有部分访问和管理权限。

3.2 密钥分量

存储密钥分量的加密机管理员卡或密封信封应在密钥监督员监督下，直接存入保险容器，且只有密钥管理员才有权取用各自生成的密钥分量。

密钥管理员调离所在机构时，应办理主密钥分量的加密机管理员卡和密封信封的交接手续，交接手续应在密钥监督员监督下进行，且应当场存入保险容器。

4. 密钥使用

4.1 票卡密钥

地市交通一卡通运营机构严格按照广东省全国交通一卡通省级平台发放的

密钥值与分散规则发行到用户卡内，票卡密钥列表详见《附录 2：广东省全国交通一卡通票卡密钥列表》。

4.2 票卡证书签发

省级交通运输主管部门负责生成和管理票卡证书所需非对称密钥对，并统一向交通运输部申请签发票卡证书。

4.3 消费密钥

存储消费业务根密钥的专用安全存取模块由省级交通一卡通运营机构统一运送至全国交通一卡通数据交换中心进行一次发卡，导入全国互通消费根密钥。

完成一次发卡后，专用安全存取模块由省级交通一卡通运营机构指定人员领回并进行省级密钥的二次发卡，完成后交付给地市交通一卡通运营机构进行发放使用。

4.4 充值密钥

省级交通运输主管部门生成和管理全省统一充值密钥，配合省级平台的 PKI 和证书两种安全体系，通过非对称密钥对算法来保障充值密钥安全。

4.4.1 PKI 体系

广东省全国交通一卡通省级平台统一发行和管理充值 PKI，依赖 PKI 安全体系，通过签到认证和加密传输来保护充值密钥安全。

4.4.2 证书体系

广东省全国交通一卡通省级平台支持第三方平台以服务形式接入，依赖证书安全体系，通过签到认证和加密传输来保护充值密钥安全。

4.5 预留密钥

省级交通运输主管部门生成和管理预留密钥，并预置于密钥载体内，用于后续业务扩展使用。

5. 密钥安全保障

5.1 安全检查

在省级交通运输主管部门的指导下，地级以上市交通运输主管部门、省级交通一卡通运营机构和地市交通一卡通运营机构定期或不定期进行密钥安全管理检查，按规定完成密钥载体维保工作，填报有关表格和报告。

5.2 密钥容灾备份

广东省全国交通一卡通省级平台采用加密方式对密钥数据进行异地备份，当故障或灾难发生导致加密机不能正常使用时，使用备份的密钥数据电子文件进行密钥数据恢复。

第二章 操作指引

第一节 加密机操作指引

1. 省级根密钥加密机

1.1 加密机初始化

当加密机要投入生产前，须完成生产初始化操作。流程包括设备初始化（加密机设备密钥分量设定和加密机管理员卡制作）、生成加密机维保密钥对、配置加密机指令白名单、导入加密机传输密钥、配置系统等。

步骤	负责角色	参与人员	项目	操作内容
1.1	加密机安全管理员	省级交通一卡通运营机构密钥管理员	前期准备	对用于加密机初始化的客户端电脑进行硬盘格式化后，安装操作系统，再安装加密机管理软件。
1.2	加密机设备管理员	省级交通运输主管部门或者省级交通一卡通运营机构密钥管理员		准备加密机设备密钥分量、加密机设备密钥分量口令和加密机管理员口令，备份于保密信封。
1.3	加密机系统管理员、加密机安全管理员、加密机审计管理员	省级交通一卡通运营机构密钥管理员		准备加密机管理员口令。
1.4	-	省级交通一卡通运营机构密钥管理员		准备加密机传输密钥分量,备份于保密信封。
2.1	加密机设备管理员	省级交通运输主管部门或者省级交通一卡通运营机构密钥管理员	设备初始化	通过加密机管理软件完成加密机设备密钥分量、加密机设备密钥分量口令和加密机管理员口令设定。
2.2	加密机安全管理员	省级交通一卡通运营机构密钥管理员		通过加密机管理软件备份加密机设备密钥数据于移动硬盘。
2.3	加密机系统管理员	省级交通一卡通运营机构密钥管理员		通过加密机管理软件设定加密机系统管理员口令。

步骤	负责角色	参与人员	项目	操作内容
2.4	加密机安全管理员	省级交通一卡通运营机构密钥管理员		通过加密机管理软件设定加密机安全管理员口令。
2.5	加密机审计管理员	省级交通一卡通运营机构密钥管理员		通过加密机管理软件设定加密机审计管理员口令。
3	加密机设备管理员	省级交通运输主管部门或者省级交通一卡通运营机构密钥管理员	生成加密机维保密钥对	通过加密机管理软件生成加密机维保密钥对，备份于移动硬盘。
4	加密机安全管理员	省级交通一卡通运营机构密钥管理员	配置指令白名单	通过加密机管理软件设定加密机指令白名单。
5	加密机安全管理员	省级交通一卡通运营机构密钥管理员	设定加密机传输密钥	通过加密机管理软件完成加密机传输密钥分量的设定。
6.1	加密机系统管理员	省级交通一卡通运营机构密钥管理员	系统配置	通过加密机管理软件完成加密机网络端口配置。
6.2	加密机系统管理员	省级交通一卡通运营机构密钥管理员		通过加密机管理软件校对加密机系统时间。

1.2 省级根密钥生成

省级根密钥加密机在为省级业务密钥加密机发放密钥前，需要通过省级平台密钥管理系统生成省级根密钥，流程包括在密钥管理系统配置省级根密钥加密机信息、配置省级根密钥信息以及密钥生成。

步骤	负责角色	参与人员	项目	操作内容
1	省级平台密钥管理系统系统配置员	省级交通运输主管部门或者省级交通一卡通运营机构密钥管理员	配置省级根密钥加密机信息	通过省级平台密钥管理系统配置省级根密钥加密机信息，分配省级平台密钥管理系统密钥管理员。
2	省级平台密钥管理系统系统密钥管理员	省级交通运输主管部门或者省级交通一卡通运营机构密钥管理员	配置省级根密钥信息	通过省级平台密钥管理系统配置省级根密钥信息。
3	省级平台密钥管理系统系统密钥管理员	省级交通运输主管部门或者省级交通一卡通运营机构密钥管理员	密钥生成	通过省级平台密钥管理系统生成省级根密钥。

1.3 加密机备份

为保障广东省全国交通一卡通加密机密钥数据安全，对密钥数据进行备份以便故障时恢复加密机密钥数据。

步骤	负责角色	参与人员	项目	操作内容
1	加密机安全管理员	省级交通一卡通运营机构密钥管理员	DES 密钥库备份	通过加密机管理软件将 DES 密钥库备份于移动硬盘。
2	加密机安全管理员	省级交通一卡通运营机构密钥管理员	SM4 密钥库备份	通过加密机管理软件将 SM4 密钥库备份于移动硬盘。
3	加密机安全管理员	省级交通一卡通运营机构密钥管理员	RSA 密钥库备份	通过加密机管理软件将 RSA 密钥库备份于移动硬盘。
4	加密机安全管理员	省级交通一卡通运营机构密钥管理员	SM2 密钥库备份	通过加密机管理软件将 SM2 密钥库备份于移动硬盘。

1.4 加密机恢复

由广东省全国交通一卡通加密机设备管理员操作，使用加密机密钥数据备份电子文件恢复加密机密钥数据。

步骤	负责角色	参与人员	项目	操作内容
1	加密机设备管理员	省级交通运输主管部门或者省级交通一卡通运营机构密钥管理员	身份认证	通过加密机管理软件认证加密机设备密钥分量口令、加密机设备管理员卡和加密机设备管理员口令。
2	加密机安全管理员	省级交通一卡通运营机构密钥管理员	设备密钥恢复	通过加密机管理软件使用加密机设备密钥备份电子文件恢复设备密钥。
3	加密机安全管理员	省级交通一卡通运营机构密钥管理员	DES 密钥库恢复	通过加密机管理软件使用密钥数据备份电子文件恢复 DES 密钥库。
4	加密机安全管理员	省级交通一卡通运营机构密钥管理员	SM4 密钥库恢复	通过加密机管理软件使用密钥数据备份电子文件恢复 SM4 密钥库。
5	加密机安全管理员	省级交通一卡通运营机构密钥管理员	RSA 密钥库恢复	通过加密机管理软件使用密钥数据备份电子文件恢复 RSA 密钥库。
6	加密机安全管理员	省级交通一卡通运营机构密钥管理员	SM2 密钥库恢复	通过加密机管理软件使用密钥数据备份电子文件恢复 SM2 密钥库。

2. 省级业务密钥加密机

2.1 加密机初始化

当广东省全国交通一卡通加密机要投入生产时，须完成生产初始化操作，流程包括设备初始化（加密机设备密钥分量设定和加密机管理员卡制作）、导入加密机维保密钥对、配置指令白名单、导入加密机传输密钥、配置系统等。

步骤	负责角色	参与人员	项目	操作内容
1.1	加密机安全管理员	省级交通一卡通运营机构密钥管理员	前期准备	对用于加密机初始化的客户端电脑进行硬盘格式化后，安装操作系统，再安装加密机管理软件。
1.2	加密机设备管理员	省级交通一卡通运营机构密钥管理员		准备加密机设备密钥分量、加密机设备密钥分量口令和加密机管理员口令，备份于保密信封。
1.3	加密机系统管理员、加密机安全管理员、加密机审计管理员	省级交通一卡通运营机构密钥管理员		准备加密机管理员口令。
1.4	-	省级交通一卡通运营机构密钥管理员		准备加密机传输密钥分量,备份于保密信封。
2.1	加密机设备管理员	省级交通一卡通运营机构密钥管理员	设备初始化	通过加密机管理软件完成加密机设备密钥分量、加密机设备密钥分量口令和加密机管理员口令设定。
2.2	加密机安全管理员	省级交通一卡通运营机构密钥管理员		通过加密机管理软件备份加密机设备密钥数据于移动硬盘。
2.3	加密机系统管理员	省级交通一卡通运营机构密钥管理员		通过加密机管理软件设定加密机系统管理员口令。
2.4	加密机安全管理员	省级交通一卡通运营机构密钥管理员		通过加密机管理软件设定加密机安全管理员口令。
2.5	加密机审计管理员	省级交通一卡通运营机构密钥管理员		通过加密机管理软件设定加密机审计管理员口令。
3	加密机设备管理员	省级交通一卡通运营机构密钥管理员	导入加密机维保密钥对	通过加密机管理软件导入加密机维保密钥对中的公钥数据。

步骤	负责角色	参与人员	项目	操作内容
4	加密机安全管理员	省级交通一卡通运营机构密钥管理员	配置指令白名单	通过加密机管理软件设定加密机指令白名单。
5	加密机安全管理员	省级交通一卡通运营机构密钥管理员	设定加密机传输密钥	通过加密机管理软件完成加密机传输密钥分量的设定。
6.1	加密机系统管理员	省级交通一卡通运营机构密钥管理员	系统配置	通过加密机管理软件完成加密机网络端口配置。
6.2	加密机系统管理员	省级交通一卡通运营机构密钥管理员		通过加密机管理软件校对加密机系统时间。

2.2 导入交通运输部密钥

按照交通运输部发布的《城市入网机构导入交通一卡通全国互联互通密钥及证书签发说明》，配合交通运输部密钥管理员完成广东省全国交通一卡通部级密钥导入。

步骤	负责角色	参与人员	项目	操作内容
1	加密机系统管理员	省级交通一卡通运营机构密钥管理员	配置网络	通过加密机管理软件配置加密机业务端口 1，IP 为 198.10.10.1，并加入 IP 白名单 192.10.10.2。
2	加密机安全管理员	省级交通一卡通运营机构密钥管理员	交通运输部初始密钥的录入	通过加密机管理软件在 0x000 索引下生成双倍长 DES 传输密钥，密钥明文为“0x11111111111111111111111111111111”，在 0x100 索引下生成 SM4 传输密钥，密钥明文为“0x11111111111111111111111111111111”。
3	交通运输部密钥管理员	交通运输部密钥管理员	交通运输部密钥导入	使用交通运输部客户端（IP：198.10.10.2）直连加密机业务端口 1，从密钥母卡将 DES 密钥和 SM4 密钥导入加密机。
4	加密机安全管理员	省级交通一卡通运营机构密钥管理员	删除交通运输部初始密钥	确认交通运输部密钥导入完成，记录导入密钥的类型及索引，通过加密机管理软件删除交通运输部传输密钥。

2.3 导入省级业务密钥

通过省级平台密钥管理系统完成广东省全国交通一卡通省级业务密钥的导入，生成用于证书签发的非对称密钥对，流程包括加密机信息配置、密钥信息配置以及密钥发行。

步骤	负责角色	参与人员	项目	操作内容
1	省级平台密钥管理系统系统配置员	省级交通一卡通运营机构密钥管理员	配置加密机信息	通过省级平台密钥管理系统配置省级业务密钥加密机信息，分配省级平台密钥管理系统密钥管理员。
2	省级平台密钥管理系统系统密钥管理员	省级交通一卡通运营机构密钥管理员	配置密钥信息	通过省级平台密钥管理系统配置省级业务密钥信息。
3	省级平台密钥管理系统系统密钥管理员	省级交通一卡通运营机构密钥管理员	密钥发行	通过省级平台密钥管理系统发行密钥。

2.4 加密机备份

为保障广东省全国交通一卡通加密机密钥数据安全，对密钥数据进行备份以便故障时恢复加密机密钥数据。

步骤	负责角色	参与人员	项目	操作内容
1	加密机安全管理员	省级交通一卡通运营机构密钥管理员	DES 密钥库备份	通过加密机管理软件将 DES 密钥库备份于移动硬盘。
2	加密机安全管理员	省级交通一卡通运营机构密钥管理员	SM4 密钥库备份	通过加密机管理软件将 SM4 密钥库备份于移动硬盘。
3	加密机安全管理员	省级交通一卡通运营机构密钥管理员	RSA 密钥库备份	通过加密机管理软件将 RSA 密钥库备份于移动硬盘。
4	加密机安全管理员	省级交通一卡通运营机构密钥管理员	SM2 密钥库备份	通过加密机管理软件将 SM2 密钥库备份于移动硬盘。

2.5 加密机恢复

由广东省全国交通一卡通加密机设备管理员操作，使用加密机密钥数据备份电子文件恢复加密机密钥数据。

步骤	负责角色	参与人员	项目	操作内容
1	加密机设备管理员	省级交通一卡通运营机构密钥管理员	身份认证	通过加密机管理软件认证加密机设备密钥分量口令、加密机设备管理员卡和加密机设备管理员口令。
2	加密机安全管理员	省级交通一卡通运营机构密钥管理员	设备密钥恢复	通过加密机管理软件使用加密机设备密钥备份电子文件恢复设备密钥。

3	加密机安全管理员	省级交通一卡通运营机构密钥管理员	DES 密钥库恢复	通过加密机管理软件使用密钥数据备份电子文件恢复 DES 密钥库。
4	加密机安全管理员	省级交通一卡通运营机构密钥管理员	SM4 密钥库恢复	通过加密机管理软件使用密钥数据备份电子文件恢复 SM4 密钥库。
5	加密机安全管理员	省级交通一卡通运营机构密钥管理员	RSA 密钥库恢复	通过加密机管理软件使用密钥数据备份电子文件恢复 RSA 密钥库。
6	加密机安全管理员	省级交通一卡通运营机构密钥管理员	SM2 密钥库恢复	通过加密机管理软件使用密钥数据备份电子文件恢复 SM2 密钥库。

3. 地市业务密钥加密机

3.1 加密机初始化

使用对应地市的广东省全国交通一卡通省级业务密钥加密机的密钥数据备份电子文件，由该加密机设备管理员复制一台地市业务密钥加密机，完成导入加密机维保密钥对、删除加密机传输密钥、配置指令白名单、重置系统管理员卡口令、配置系统等操作。

步骤	负责角色	参与人员	项目	操作内容
1	加密机设备管理员	省级交通一卡通运营机构密钥管理员	加密机初始化	使用加密机管理软件，由加密机设备管理员操作，复制对应地市的地市业务密钥加密机。
2	加密机设备管理员	省级交通一卡通运营机构密钥管理员	导入加密机维保密钥对	通过加密机管理软件导入加密机维保密钥对中的公钥数据。
3	加密机安全管理员	省级交通一卡通运营机构密钥管理员	删除加密机传输密钥	通过加密机管理软件删除加密机传输密钥。
4	加密机安全管理员	省级交通一卡通运营机构密钥管理员	配置指令白名单	通过加密机管理软件设定加密机指令白名单。
5	加密机系统管理员	省级交通一卡通运营机构密钥管理员	重置系统管理员卡口令	通过加密机管理软件将加密机系统管理员口令重置为8位发卡机构代码(例：韶关为“02885820”)。
5.1 (可选)	加密机设备管理员、安全管理员、审计管理员	省级交通一卡通运营机构密钥管理员	重置其他管理员卡口令	通过加密机管理软件将加密机设备管理员、安全管理员、审计管理员口令重置为 8 位发卡机构代码（例：韶关为“02885820”)。需交付以上管理员卡时进行此操作。

6	加密机审计管理员	省级交通一卡通运营机构密钥管理员	系统配置	通过加密机管理软件校对加密机系统时间。

3.2 配置加密机维保信息

由省级交通一卡通运营机构完成广东省全国交通一卡通地市业务密钥加密机维保信息的配置工作，维保信息由省级或者地级以上市交通运输主管部门视实际情况设定。

步骤	负责角色	参与人员	项目	操作内容
1	省级平台密钥管理系统系统密钥管理员	省级交通一卡通运营机构密钥管理员	申请维保	通过加密机维保客户端生成维保信息申请电子文件。
2	省级平台密钥管理系统系统密钥管理员、加密机安全管理员	省级交通一卡通运营机构密钥管理员	导入维保信息电子文件	加密机安全管理员通过加密机管理软件进行登录验证，省级平台密钥管理系统密钥管理员将维保信息申请电子文件导入省级平台密钥管理系统。
3	省级平台密钥管理系统系统密钥管理员、加密机安全管理员	省级交通一卡通运营机构密钥管理员	生成维保信息更新电子文件	加密机安全管理员通过加密机管理软件进行登录验证，省级平台密钥管理系统密钥管理员配置以下维保更新信息，并生成维保信息更新电子文件 电子钱包圈存密钥 UB 指令（MAC/TAC 计算）x 次和有效期 y。 电子钱包 TAC 密钥 UB 指令（MAC/TAC 计算） x 次和有效期 y。 电子现金发卡行私钥 EH 指令（导出非对称私钥） x 次和有效期 y。 电子钱包圈存密钥 U1 指令（加解密计算）和 U3 指令（安全报文方式导出对称密钥） n 次和有效期 m。 电子钱包 TAC 密钥 U1 指令（加解密计算）和 U3 指令（安全报文方式导出对称密钥）n 次和有效期 m。 电子钱包消费密钥 U1 指令（加解密计算）和 U3 指令（安全报文方式导出对称密钥）n 次和有效期 m。 电子现金 MAC 密钥 U1 指令（加解密计算）和 U3 指令（安全报文方式导出对称密钥） n

步骤	负责角色	参与人员	项目	操作内容
				次和有效期 m。 电子现金 AC 密钥 U1 指令（加解密计算）和 U3 指令（安全报文方式导出对称密钥） n 次和有效期 m。 **注 n、m、x 与 y 由省级或者地级以上市交通运输主管部门视实际情况设定。*
4	省级平台密钥管理系统系统密钥管理员	省级交通一卡通运营机构密钥管理员	导入维保信息更新电子文件	通过加密机维保客户端导入维保信息更新电子文件。 详见《附录 3：地市业务密钥加密机指令白名单》
5	加密机系统管理员	省级交通一卡通运营机构密钥管理员	确认维保信息更新正确	通过加密机维保客户端与加密机管理软件确认维保信息更新正确。

3.3 加密机维保信息更新

地市业务密钥加密机管理员发起维保申请，省级平台按照安全策略审核维保信息电子文件并生成维保信息更新电子文件。省级平台将维保信息更新电子文件回复给地市业务密钥加密机管理员完成加密机维保信息更新。

步骤	负责角色	参与人员	项目	操作内容
1	省级平台密钥管理系统系统密钥管理员	省级或地级以上市交通运输主管部门密钥管理人员	申请维保	省级平台密钥管理系统系统密钥管理员接收地市业务密钥加密机管理员维保信息申请电子文件与《广东省全国交通一卡通加密机维保申请表》（详见《附录 4：广东省全国交通一卡通加密机维保申请表》）。
2	省级平台密钥管理系统系统密钥管理员、加密机安全管理员	省级或地级以上市交通运输主管部门密钥管理人员	导入维保信息电子文件	加密机安全管理员通过加密机管理软件进行登录验证，省级平台密钥管理系统密钥管理员将维保信息申请电子文件导入省级平台密钥管理系统。
3	省级平台密钥管理系统系统	省级或地级以上市交通运输	生成维保信息更新电子文件	加密机安全管理员通过加密机管理软件进行登录验证，省级平台密钥管理系统密钥管理员配置以下维保更新信息，并生成维保信

步骤	负责角色	参与人员	项目	操作内容
	密钥管理员、加密机安全管理员	主管部门密钥管理人员		息更新电子文件 电子钱包圈存密钥 UB 指令（MAC/TAC 计算） x 次和有效期 y。 电子钱包 TAC 密钥 UB 指令（MAC/TAC 计算） x 次和有效期 y。 电子现金发卡行私钥 EH 指令（导出非对称私钥） x 次和有效期 y。 电子钱包圈存密钥 U1 指令（加解密计算）和 U3 指令（安全报文方式导出对称密钥）n 次和有效期 m。 电子钱包 TAC 密钥 U1 指令（加解密计算）和 U3 指令（安全报文方式导出对称密钥）n 次和有效期 m。 电子钱包消费密钥 U1 指令（加解密计算）和 U3 指令（安全报文方式导出对称密钥）n 次和有效期 m。 电子现金 MAC 密钥 U1 指令（加解密计算）和 U3 指令（安全报文方式导出对称密钥）n 次和有效期 m。 电子现金 AC 密钥 U1 指令（加解密计算）和 U3 指令（安全报文方式导出对称密钥）n 次和有效期 m。 **注 n、m、x 与 y 由省级或者地级以上市交通运输主管部门视实际情况设定。*
4	省级平台密钥管理系统系统密钥管理员	省级或地级以上市交通运输主管部门密钥管理人员	省级平台密钥管理系统密钥管理员	将维保信息更新电子文件回复给地市业务密钥加密机管理员。

第二节 密钥数据备份指引

为有效控制风险及保障密钥安全，广东省全国交通一卡通加密机设备密钥分量备份、加密机设备密钥分量口令备份、加密机管理员口令备份等备份数据须分开保管，具体实施如下：

1. 省级交通运输主管部门安全保密地点

省级交通运输主管部门安排 3 个保密地点，每个保密点需要至少两名密钥管理员才能领取相关物品，且每次仅能领取 1 样物品。

2. 省级交通一卡通运营机构安全保密地点

省级交通一卡通运营机构安排 3 个保密地点，每个保密点需要至少两名密钥管理员才能领取相关物品，且每次仅能领取 1 样物品。

3. 管理员卡管理

加密机管理员卡及加密机管理员口令由管理员本人独立保管，严禁交予他人使用。

附录 1：广东省全国交通一卡通入网发卡机构信息

名称	城市代码	卡片 IIN 号(扩展)	公钥证书申请记录号	发卡机构代码
广州市	5810	310487(03)	000099	02205810
深圳市	5840	310487(04)	000100	02215840
中山市	6030	310487(05)	000101	01056030
珠海市	5850	310487(24)	000102	01355850
东莞市	6020	310487(02)	000103	01616020
佛山市	5880	310487(07)	000183	02775880
惠州市	5950	310487(08)	000184	02785950
汕头市	5860	310487(09)	000185	02795860
江门市	5890	310487(10)	000186	02805890
茂名市	5920	310487(11)	000187	02815920
肇庆市	5930	310487(12)	000188	02825930
湛江市	5910	310487(13)	000189	02835910
梅州市	5960	310487(14)	000190	02845960
汕尾市	5970	310487(15)	000191	02855970
河源市	5980	310487(16)	000192	02865980
清远市	6010	310487(17)	000193	02876010
韶关市	5820	310487(18)	000194	02885820
揭阳市	6050	310487(19)	000195	02896050
阳江市	5990	310487(20)	000196	02905990
潮州市	6040	310487(21)	000197	02916040
云浮市	6060	310487(22)	000198	02926060

*注：以上地市按发卡机构公钥证书申请记录号的先后排序，按实际情况更新。

附录 2：广东省全国交通一卡通票卡密钥列表

密钥用途	说明
应用维护密钥_01	一级分散后发放，用于入网机构所发行的用户卡电子钱包应用的复合交易文件修改。
应用维护密钥_02	一级分散后发放，用于入网机构所发行的用户卡电子钱包应用的交通部、省内卡信息专用文件修改。
应用维护密钥_03	一级分散后发放，用于入网机构所发行的用户卡电子钱包应用省内交易复合文件修改。
消费密钥_01	一级分散后发放，用于入网机构所发行的用户卡电子钱包应用消费密钥。
消费密钥_02	一级分散后发放，用于入网机构所发行的用户卡电子钱包应用消费密钥。
圈存密钥_01	一级分散后发放，用于入网机构所发行的用户卡电子钱包应用充值密钥。
圈存密钥_02	一级分散后发放，用于入网机构所发行的用户卡电子钱包应用充值密钥。
圈存密钥_03	一级分散后发放，用于入网机构所发行的用户卡电子钱包应用充值密钥。
TAC 密钥	一级分散后发放,用于入网机构所发行的用户卡电子钱包应用 TAC 密钥。
应用锁定密钥	一级分散后发放，用于入网机构所发行的用户卡应用锁定。
应用解锁密钥	一级分散后发放，用于入网机构所发行的用户卡应用解锁。
外部认证密钥_01	一级分散后发放，用于入网机构所发行的用户卡电子钱包应用文件创建。
外部认证密钥_02	一级分散后发放，用于入网机构所发行的用户卡电子钱包应用认证。
外部认证密钥_03	一级分散后发放，用于入网机构所发行的用户卡电子钱包应用敏感信息读写权限。

圈提密钥	一级分散后发放，用于入网机构所发行的用户卡电子钱包应用圈提。
修改透支限额密钥	一级分散后发放，用于入网机构所发行的用户卡电子钱包应用修改透支限额。
应用密文密钥（AC）	一级分散后发放，用于入网机构所发行的用户卡电子现金应用 AC 密钥。
互通记录保护密钥-电子现金	一级分散后发放，用于入网机构所发行的用户卡电子现金应用的行业扩展应用文件修改。
安全报文认证密钥（MAC）	一级分散后发放，用于入网机构所发行的用户卡电子现金应用 MAC 密钥。
安全报文加密密钥（ENC）	一级分散后发放，用于入网机构所发行的用户卡电子现金应用 ENC 密钥。
省级扩展应用开通密钥	一级分散后发放，用于入网机构所发行的用户卡电子现金应用的行业扩展应用文件开通。
省级扩展应用管理密钥_01	一级分散后发放，用于入网机构所发行的用户卡电子现金应用的行业扩展应用文件修改。
省级扩展应用管理密钥_02	一级分散后发放，用于入网机构所发行的用户卡电子现金应用的行业扩展应用文件修改。

附录 3：地市业务密钥加密机指令白名单

指令	说明
NC	密机诊断
TE	产生随机数
EI	产生非对称密钥对
EJ	从私钥获取公钥
EH	导出非对称私钥
EP	私钥解密运算
ER	公钥加密运算
GM	计算数据摘要
UB	计算及校验 MAC/TAC
KW	算法 ARQC/TC/ACC 校验，ARPC 产生
G1	产生安全通道会话密钥
U1	分散密钥数据加解密计算
U3	安全报文方式导出对称密钥

附录 4：广东省全国交通一卡通加密机维保申请表

发卡机构代码		**加密机编号**	
加密机序列号			
申请单位			
申请人		**申请日期**	
申请单位地址			
申请单位电话号码			
上次维保时间			
本年度票卡发行量			
下年度计划票卡发行量			
备注			
申请单位（公章）： 日期：			