附件1

**广东省全国交通一卡通密钥说明**

广东省全国交通一卡通密钥包括部级密钥、省级密钥和地市根据业务需要发行的本地密钥。其中部级密钥按密码算法可分为对称密钥和非对称密钥，部级对称密钥由交通运输部按地市机构代码分散后进行下发，部级非对称密钥由省厅统一生成证书后交由交通运输部签发后下发。省级密钥包括省内充值密钥、省内互通密钥、省内主控密钥和省内维护密钥，省级密钥由省厅按地市机构代码分散后下发。地市本地密钥，由地市交通运输主管部门根据地方业务需要，进行发行和使用。

广东省全国交通一卡通密钥按部、省、市三级模式进行发行和管理，具体说明如下：

一、框架结构图



二、密钥说明

交通部运输部《城市公共交通IC卡技术规范》（JT/T 978-2015）包括电子钱包标准和电子现金标准，其中电子钱包和电子现金对称密钥说明如下：

（一）电子钱包密钥说明

|  |  |  |
| --- | --- | --- |
| **序号** | **密钥名称** | **密钥来源** |
| 1 | 应用主控子密钥 | 省交通运输厅 |
| 2 | 应用维护子密钥\_00 | 省交通运输厅 |
| 3 | 应用维护子密钥\_01 | 交通运输部 |
| 4 | 应用维护子密钥\_02 | 省交通运输厅 |
| 5 | 应用维护子密钥\_03 | 省交通运输厅 |
| 6 | 消费子密钥\_01 | 交通运输部 |
| 7 | 消费子密钥\_02 | 省交通运输厅 |
| 8 | 圈存子密钥\_01 | 省交通运输厅 |
| 9 | 圈存子密钥\_02 | 省交通运输厅 |
| 10 | 圈存子密钥\_03 | 省交通运输厅 |
| 11 | TAC 子密钥 | 交通运输部 |
| 12 | 应用锁定子密钥 | 交通运输部 |
| 13 | 应用解锁子密钥 | 省交通运输厅 |
| 14 | 外部认证子密钥\_01 | 省交通运输厅 |
| 15 | 外部认证子密钥\_02 | 省交通运输厅 |
| 16 | 外部认证子密钥\_03 | 省交通运输厅 |
| 17 | 圈提密钥\_01 | 省交通运输厅 |
| 18 | 修改透支限额密钥 | 省交通运输厅 |

（二）电子现金密钥说明

|  |  |  |
| --- | --- | --- |
| 序号 | 密钥名称 | 密钥来源 |
| 1 | 应用密文主密钥（AC） | 交通运输部 |
| 2 | 安全报文认证密钥（MAC） | 省交通运输厅 |
| 3 | 安全报文加密密钥（ENC） | 省交通运输厅 |
| 4 | 省级扩展应用开通密钥 | 省交通运输厅 |
| 5 | 省级扩展应用管理密钥\_01 | 省交通运输厅 |
| 6 | 省级扩展应用管理密钥\_02 | 省交通运输厅 |

附件2

**广东省全国交通一卡通密钥使用模式说明**

广东省全国交通一卡通密钥按使用方式可分为票卡发行密钥和终端使用密钥，票卡发行密钥采用定制加密机的灌装形式下发，终端使用密钥采用PSAM/PKI卡的灌装形式下发。各地市交通运输主管部门根据地市一卡通运营主体的情况选择省级中心集中发卡或地市自主发卡，对应的密钥管理模式为集中托管模式或自主使用模式。

一、密钥集中托管模式

省级管理平台技术上支持地市一卡通运营主体部署定制加密机（存储传输密钥），实现由地市一卡通运营主体的本地发行写卡，同时也支持通过省级管理平台的集中发行写卡。采用集中发行写卡方式的地市一卡通运营主体，在地市管理平台不用部署票卡发行的相关设备（加密机、票卡发行机、票卡读写设备等）和软件（数据准备系统、票卡发行系统等），同时不用为票卡发行工作配备相关的运维人员。



二、密钥自主使用模式

地市一卡通运营主体部署的定制加密机存储部级密钥、省级密钥，并部署用于票卡发行工作的相关设备（票卡发行机、票卡读写设备等）和软件（数据准备系统、票卡发行系统等）及与之相关的运维人员。地市一卡通运营主体自行组织相关软件的设计、开发和运维工作，定制的加密机接受省厅的定期或不定期审验。



附件3

**全国交通一卡通密钥（加密机）申请表**

(式样)

广东省交通运输厅 :

为贯彻落实部《关于促进交通一卡通健康发展加快实现互联互通的指导意见》（交运发〔2015〕65 号）和《广东省交通运输厅关于印发<广东省公共交通一卡通管理办法>的通知》（粤交运〔2016〕130号）的文件要求，更好地推进我市全国交通一卡通互联互通工作，现申请领用 市全国交通一卡通密钥（加密机）。

我局（委）承诺：严格按照国家和省内有关密码管理使用规定，做好各单位全国交通一卡通密钥（加密机）使用的监管工作，落实安全责任，保证全国交通一卡通密钥（加密机）管理安全。

附件：全国交通一卡通密钥（加密机）管理信息联络表

单位公章

年 月 日

 (联系人 : 电话: )

**全国交通一卡通密钥（加密机）管理信息联络表**

|  |  |
| --- | --- |
| 申请单位  |  |
| 联系人 |  | 联系电话 |  |
| 负责人 |  | 联系电话 |  |
| 办公传真 |  | 电子邮箱 |  |
| 申请类型 | □密钥集中托管 □密钥自主使用 |
| 安全人员 | 姓名 | 性别 | 联系电话 | 身份证号码 | 备注 |
|  |  |  |  | 见涉密人员审查登记表 |
|  |  |  |  |  |
|  |  |  |  |  |
| 用途说明 |  |
| 地市交通运输局委审核意见 |  |
| 单位签章： |
| 日 期： 年 月 日 |
| 省交通运输厅意见 | 批复： |
| 审批人： |
| 日 期： 年 月 日 |

**涉密人员审查登记表**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 姓名 |  | 性别 |  | 出生年月 |  | 文化程度 |  | 免冠一寸照片 |
| 政治面貌 |  | 民族 |  | 籍贯 |  |
| 毕业院校 |  | 所学专业 |  |
| 参加工作时间 |  | 公司工作时间 |  | 职务职称 |  | 涉密级别 |  |
| 家庭住址 |  | 联系手机 |  |
| 身份证号码 |  | 住宅电话 |  |
| 家庭主要成员 | 姓名 | 称谓 | 年龄 | 政治面貌 | 职业 | 工作单位及地址 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| 主要社会关系情况 | 姓名 | 称谓 | 年龄 | 政治面貌 | 职业 | 工作单位及地址 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| 直系亲属在境外情况 | 姓名 | 称谓 | 年龄 | 政治面貌 | 职业 | 所在国家、地区及住址 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

附件4

**广东省全国交通一卡通PSAM/PKI卡申请表**

(式样)

广东岭南通股份有限公司：

我司因开通全国交通一卡通及岭南通互联互通业务需要，现向贵司申领以下密钥管理卡：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 产品名称 | 规格型号 | 数量（张） | 备注 |
| 1 | 部省兼容PSAM卡 | 正式密钥 |  |  |
| 2 | 岭南通PKI卡 | 正式密钥 |  |  |
|  | 合计 |  |  |  |

我司承诺，妥善保管所申领的密钥管理卡，保证归还时设备处于可正常使用的状态。如因我司原因造成所申领的密钥管理卡丢失或损毁，我司承诺赔偿由此造成的经济损失。专此函达。

附件：应用网点列表

（公章）

年 月 日

(联系人 : 电话: )

附件

**PKI卡应用网点列表**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 网点名称 | 应用区域（详细地址） | 网点数量（个） | 所用设备品牌 | 设备型号 |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |
| 3 |  |  |  |  |  |
| 4 |  |  |  |  |  |
| 合计 |  |  |  |

附件

**PSAM卡应用网点列表**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 线路名称 | 始发站-终点站 | 应用车辆牌号 | 应用数量（个） | 所用设备品牌 | 设备型号 |
| 1 |  |  |  |  |  |  |
|  |
|  |
|  |
| 2 |  |  |  |  |  |  |
|  |
|  |
|  |
| 3 |  |  |  |  |  |  |
|  |
|  |
|  |
| 4 |  |  |  |  |  |  |
|  |
|  |
|  |
|  | 合计 |  |  |  |  |  |