ICS 03.220.20;35.240.60
R 10
备案号:

JT

中华人民共和国交通运输行业标准

JT/T 825.8—2012

IC卡道路运输证件
第8部分:密钥安全体系框架

IC card license for road transportation—
Part 8:Security architecture of keys

2012-02-20 发布　　2012-05-01 实施

中华人民共和国交通运输部　发布

目　　次

前　言

JT/T 825《IC 卡道路运输证件》分为 13 个部分：

——第 1 部分：总体技术要求；

——第 2 部分：IC 卡技术要求；

——第 3 部分：IC 卡道路运输证数据格式；

——第 4 部分：IC 卡道路运输证规格与样式；

——第 5 部分：IC 卡从业资格证数据格式；

——第 6 部分：IC 卡从业资格证规格与样式；

——第 7 部分：IC 卡物理防伪膜技术要求；

——第 8 部分：密钥安全体系框架；

——第 9 部分：密钥管理系统技术要求；

——第 10 部分：IC 卡初始化设备技术要求；

——第 11 部分：IC 卡证卡打印机技术要求；

——第 12 部分：IC 卡读写器技术要求；

——第 13 部分：IC 卡及关键设备检测规范。

本部分为 JT/T 825 的第 8 部分。

本部分按照 GB/T 1.1—2009 给出的规则起草。

本部分由交通运输部信息通信及导航标准化技术委员会提出并归口。

本部分主要起草单位：交通运输部公路科学研究院、交通运输部科学研究院。

本部分参加起草单位：广东省交通运输厅、山西省交通运输管理局、甘肃省公路运输管理局。

本部分主要起草人：吴金中、张永军、杨富峰、陈宓、郑晓峰、刘志、宋伟、陈永峰。

IC卡道路运输证件
第8部分:密钥安全体系框架

1 范围

JT/T 825的本部分规定了IC卡道路运输证件有关密钥安全的总体框架,以及密钥管理、使用相关技术要求。

本部分适用于IC卡道路运输证件密钥管理及安全认证体系。

2 总体框架

2.1 框架结构

IC卡道路运输证件密钥体系采用部省两级管理的模式,总体框架如图1所示。

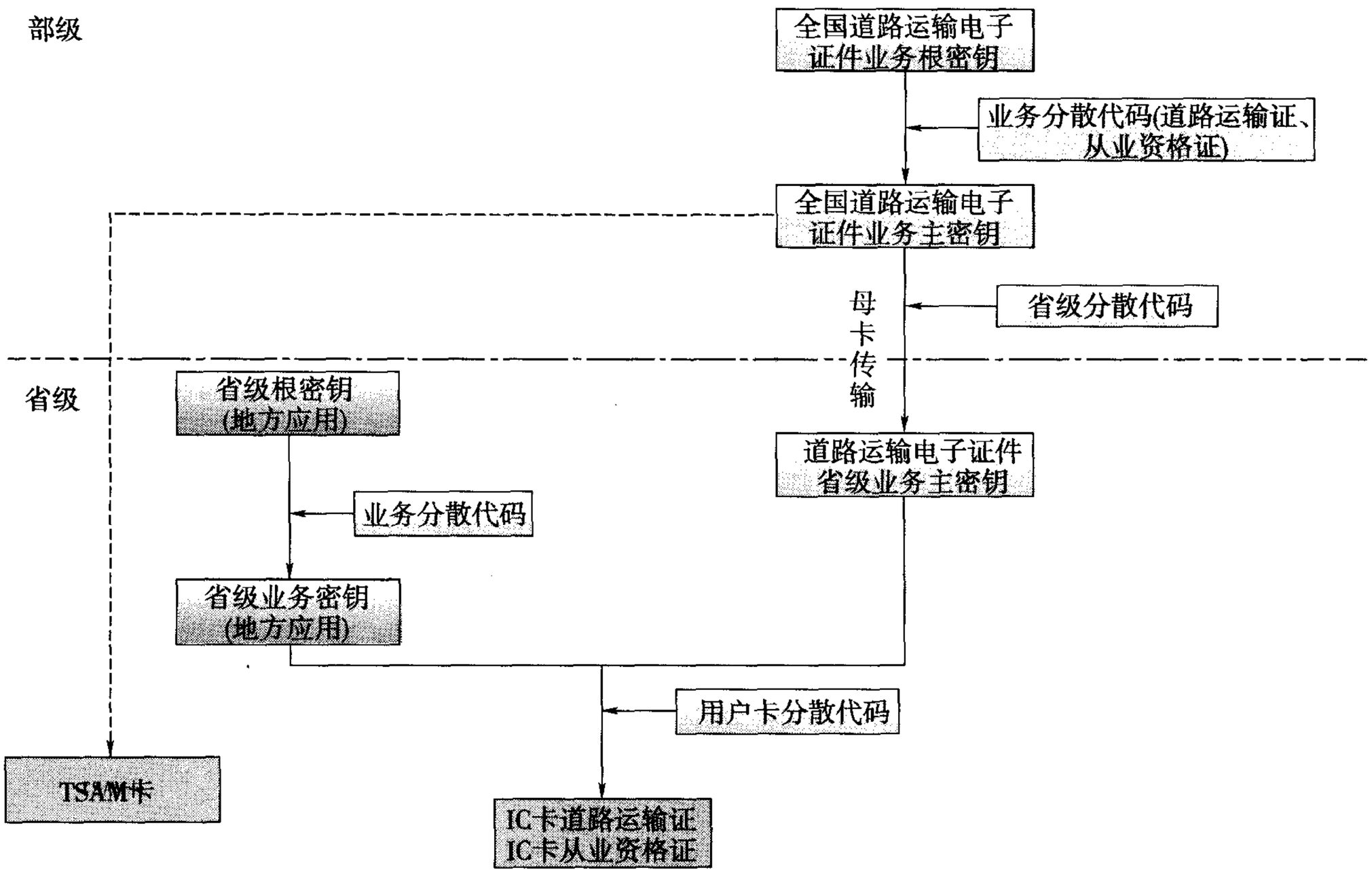

图1 总体框架

2.2 全国道路运输电子证件业务根密钥

作为全国道路运输电子证件业务应用的总密钥,由交通运输行业总控密钥根据一定规则分散产生。通过全国道路运输电子证件业务根密钥可分散产生全国道路运输电子证件业务主密钥、卡片控制密钥等。

2.3 全国道路运输电子证件业务主密钥

主要包括道路运输电子证件全国通读通写的密钥,如IC卡道路运输证真伪认证密钥、IC卡道路运输

证省外稽查业务应用密钥、IC 卡从业资格证真伪认证密钥、IC 卡从业资格证省外稽查业务应用密钥等。全国道路运输电子证件业务主密钥由全国道路运输电子证件业务根密钥根据相关业务代码分散生成。全国道路运输电子证件业务主密钥在下发到各省的同时，也灌装到 TSAM 卡中。

2.4 道路运输电子证件省级业务主密钥

涉及道路运输电子证件全国通读通写的密钥，由全国道路运输电子证件业务主密钥经省级分散代码分散生成，并在省级层面二次分散后灌装到 IC 卡道路运输证、IC 卡从业资格证。

2.5 省级根密钥

作为各省道路运输电子证件地方应用的总密钥，由各省根据一定规则自行产生。通过省级根密钥可分散产生省级业务密钥、卡片控制密钥等。

2.6 省级业务密钥

主要包括道路运输电子证件地方应用相关密钥，如年审管理写密钥，客运班车进站管理应用密钥等。省级业务密钥由省级根密钥依据相关业务代码分散生成，并按照用户卡分散代码分散后灌装到 IC 卡道路运输证、IC 卡从业资格证。

3 密钥管理的安全要求

3.1 密钥生成

密钥生成过程应保证所生成密钥的机密性、安全性、随机性，密钥生成过程应确保不可预测。在密钥生成时，应采取以下措施：

a） 密钥生成采用硬件加密的方式；

b） 传输密钥应采用不可重复的方式生成；

c） 密钥生成的环境应保证安全；

d） 密钥生成过程应严格按照安全的操作规程进行。

3.2 密钥的下发

根据密钥的用途，业务密钥采用逐级下发的方式，即由上一级生成下一级所需的子密钥，并保存在密钥母卡及密钥传输控制卡中传递给下一级。

3.3 密钥存储

密钥不能以明文方式存储在安全存储设备之外。

可采取下列一项或多项措施防止存储密钥被篡改和非授权替换：

a） 从物理或逻辑上防止对密钥存储区的非授权访问；

b） 根据不同的使用目的将密钥加密后存储；

c） 确保不能同时知道明文数据及其密文数据。

3.4 密钥备份

密钥备份应以密文的方式存储到卡片或密钥管理设备中。密钥备份过程应保证密钥不被泄露、替换和篡改。

密钥备份后的存储设备应采用多人分开保管的形式。

3.5 密钥恢复

通过备份设备将密钥恢复到密钥系统安全设备中。

密钥恢复应当经过授权,并严格遵循安全规章制度。

3.6 密钥更新

当密钥的生命周期结束或系统的密钥泄露后,需要进行密钥的更新。密钥更新的基本原则是:保护持卡人的利益不受损害,不影响持卡人的正常使用;密钥更新是不可逆的,被更新的密钥应被归档或销毁,与更新密钥存在管理的其他密钥应一并更新;密钥更新的全过程应保证系统的安全性能不受影响。

每组密钥应有有效期,有效期过后系统须启用新版本的密钥组,并用于发行新卡。在卡片生命周期或当前使用的密钥泄露的紧急情况下,启用不同的版本密钥。

3.7 密钥销毁

密钥销毁是安全删除不再使用的密钥,包括销毁所有已归档和备份的密钥。在密钥销毁后,不应有任何信息可以用来恢复已销毁的密钥。

4 密钥使用安全技术要求

密钥使用安全技术要求如下:

a) 不同的应用应使用不同的密钥;

b) 密钥不允许以明文方式直接读;

c) 密钥应在主控密钥的控制下更新;

d) 密钥应不能被外界直接访问,只能接受内部系统的操作。