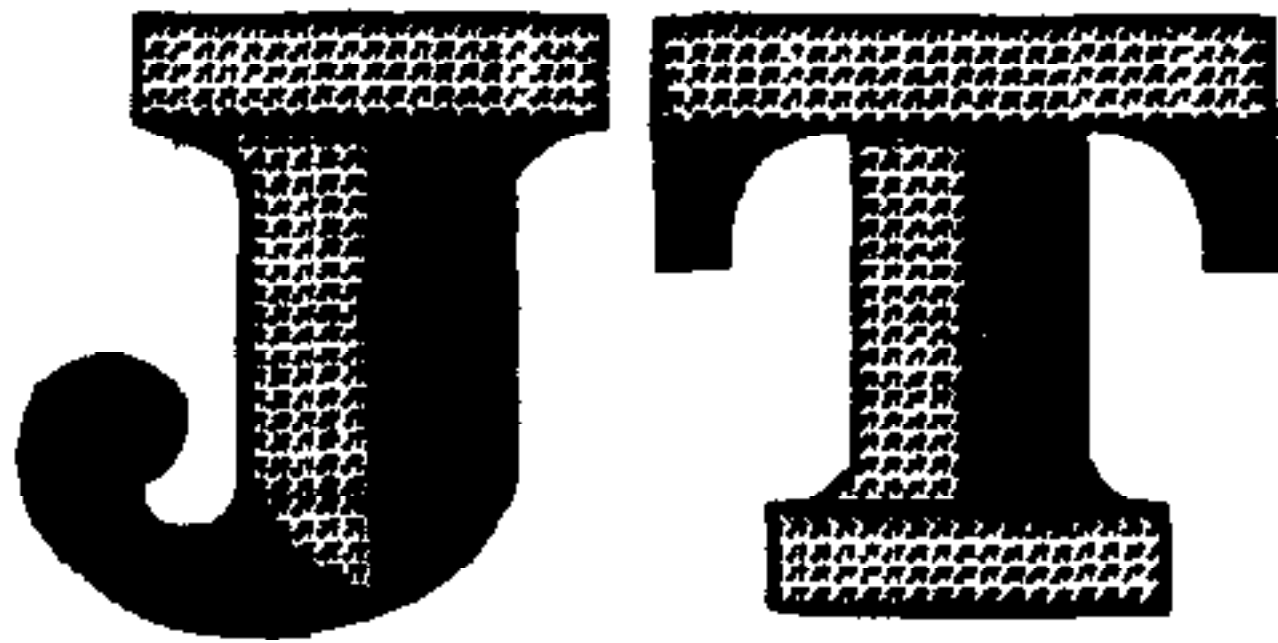


ICS 03.220.20;35.240.60

R 10

备案号:



中华人民共和国交通运输行业标准

JT / T 825.9—2012

IC 卡道路运输证件 第 9 部分:密钥管理系统技术要求

IC card license for road transportation—
Part 9: Requirements for keys management system

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 124

1 范围 125

2 总体要求 125

3 功能要求 125

4 技术要求 125

5 运行环境要求 126

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 9 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、林海、郑晓峰、彭美华、宋伟、陈永峰。

IC 卡道路运输证件

第 9 部分：密钥管理系统技术要求

1 范围

JT/T 825 的本部分规定了 IC 卡道路运输证件部省两级密钥管理系统的功能和技术要求。
本部分适用于 IC 卡道路运输证件部省两级密钥管理系统的建设和使用。

2 总体要求

省级密钥管理系统应通过与部级密钥管理系统的兼容性测试,确保部省两级密钥管理体系的安全性、兼容性和可靠性。

3 功能要求

3.1 部级密钥管理系统

部级密钥管理系统负责产生 IC 卡道路运输证件中全国通读通写应用的密钥(如证件认证、跨省稽查等),为省级密管系统产生对应的子密钥,并以安全的方式传输到各省市。

主要功能是:

- a) 为道路运输管理业务生成全国性根密钥,所有的全国道路运输电子证件业务主密钥均由此分散,在密钥体系上保证了 IC 卡的全国互认;
- b) 在全国业务主密钥的基础上,为各省分散不同的业务主密钥,并通过密钥母卡及密钥传输控制卡的形式下发给各省市;
- c) 全国通读通写密钥的管理,包括密钥生成、密钥下发、密钥存储、密钥备份、密钥恢复、密钥销毁等;
- d) 为 TSAM 卡的一次发行提供密钥支持。

3.2 省级密钥管理系统

省级密钥管理系统通过部级密钥管理系统下发的密钥母卡和密钥传输控制卡,获得经过分散的全国道路运输证件业务主密钥,生成本地基本、扩展应用所需要的密钥。

主要功能是:

- a) 从部级密钥管理系统领取经分散后的全国道路运输电子证件业务主密钥,即道路运输电子证件省级业务主密钥(简称“二级密钥”),并导入到省级密钥管理系统中;
- b) 为本省道路运输管理业务生成省级根密钥,省内所有的地方应用密钥均由此分散;
- c) 为本省发行用户卡(IC 卡道路运输证、IC 卡从业资格证)、TSAM 卡的二次发行提供密钥支持;
- d) 本省应用密钥管理,包括密钥生成、密钥存储、密钥备份、密钥恢复、密钥销毁等。

4 技术要求

4.1 密钥管理系统加密功能应通过硬件加密机实现。

- 4.2 密钥管理系统中的密钥可灵活定义和配置。
- 4.3 后续增加的密钥不应影响先前已生成的密钥。
- 4.4 密钥管理系统可通过领导卡生成根密钥并分散出所需应用密钥。

5 运行环境要求

- 5.1 密钥管理系统应运行在一个独立的封闭式网络中。
 - 5.2 部署密钥管理系统的机房应配有双重身份认证门禁系统、24h 监控系统、不间断电源设备及设备专用机柜等,推荐使用屏蔽机房。
 - 5.3 密钥加密机应获得国家密码管理部门颁发的商用密码产品型号证书。
-