高速公路区域联网不停车收费示范工程暂行技术要求 第 1 部分

密钥管理规则

2008 年 8 月

第一章　总　则

第一条　为加强收费公路非现金支付IC卡密钥统一管理，保证收费公路非现金支付的安全性，根据《收费公路联网收费技术要求》的规定及有关技术标准，制定本规则。

第二条　公路电子收费密钥分为国家密钥和省级密钥。

第三条　凡为开展收费公路非现金支付业务的密钥管理必须遵守本规则。

第四条　本规则所称用户 IC 卡是指在中华人民共和国境内使用的向社会公开发行的具有收费公路通行费缴纳功能的智能卡；密钥是指对用户 IC 卡信息进行加密变换的保密数据；PSAM 卡是指收费公路收费终端设备的安全访问模块；ESAM 模块是指不停车收费车载单元的安全访问模块。

第二章　国家密钥管理

第五条　国家密钥由国务院交通运输主管部门负责管理。具体工作由其委托的单位承担。

第六条　国家密钥管理的主要内容是：

（一）制作及管理全国消费主密钥；

（二）分发、管理省级密钥母卡和传输卡；

（三）分发、管理PSAM卡和ESAM模块；

（四）指导省级密钥管理系统的建设和运营；

（五）其他工作。

第三章　省级密钥管理

第七条　省级密钥由省级交通主管部门负责管理。具体工作可由其委托的单位承担，但应确保其唯一性。

第八条　省级密钥管理的主要内容是:

（一）按照附件一的要求建设省级密钥管理系统并负责维护;

（二）制作及管理各类最终应用密钥;

（三）申领省级密钥母卡、传输卡，和PSAM卡;

（四）发放和管理本辖区内各种密钥母卡、PSAM卡、用户IC卡，并对上述卡进行使用注册登记和监控管理;

（五）其他工作。

第九条　省级交通主管部门应按照附件二的要求向国务院交通运输主管部门申请省级密钥母卡和传输卡。

第十条　获得批准后，省级交通主管部门应派专人持批复函件，向国家密钥管理承担单位领取省级密钥母卡及传输卡。

第十一条 省级密钥管理承担单位应妥善保管省级密钥母卡及传输卡，母卡内密钥仅限于导入本省密钥管理系统。

第十二条 在操作、使用过程中损坏的密钥母卡和传输卡，省级密钥管理承担单位应如数及时退回国家密钥管理承担单位统一销毁。

第四章　PSAM卡的发放和管理

第十三条 装有正式密钥的PSAM卡仅限省级密钥管理承担单位申请领用。但对于测试、试验所需的PSAM卡，可由其他企、事业单位申请领用。

第十四条 申领单位向国家密钥管理承担单位领取《公路电子收费PSAM卡申请表》(样表见附件三)，填写并盖章后，递交至国家密钥管理承担单位。

第十五条 国家密钥管理承担单位应在3个工作日内对所提交的材料进行审核，并在5个工作日内制作完成PSAM卡。

第十六条 接到国家密钥管理承担单位同意通知后，申请单位应派专人领取装有正式密钥的PSAM卡。

第十七条 省级密钥管理承担单位对使用过程中损坏的PSAM卡应如数退回国家密钥管理承担单位统一销毁。PSAM卡如有丢失，省级密钥管理承担单位应在2个工作日内以书面形式上报至国家密钥管理承担单位。

第五章　ESAM模块的发放和管理

第十八条 国家密钥管理承担单位负责对电子收费车载单元的ESAM模块进行初始化。

第十九条 申请单位应向国家密钥管理承担单位领取《公路电子收费ESAM申请表》(样表见附件四)，填写并盖章后，连同企业营业执照复印件一起递交至国家密钥管理承担单位。

第二十条 国家密钥管理承担单位应在3个工作日内对所提交的材料进行审核，并在15个工作日内制作完成ESAM模块。

第二十一条 接到国家密钥管理承担单位同意通知后，申请单位应派专人领取ESAM模块。

第六章 支持与服务

第二十二条 国家密钥管理承担单位应向省级密钥管理承担单位提供PSAM卡及省级密钥母卡、传输卡使用说明及接口资料，并协助调试，同时协调组织对省级密钥管理人员进行技术培训。

第二十三条 国家密钥管理承担单位应积极配合省级密钥管理系统的建设，并根据省级密钥管理承担单位的需要提供相关增值服务。

第二十四条 消费主密钥一般每三年更新一次。如有特殊需要，国务院交通运输主管部门有权随时更换全国消费主密钥。

第七章 附则

第二十五条 本规则由国务院交通运输主管部门负责解释。

第二十六条 本规则从发布之日起开始执行。

附件一:

省级密钥管理系统建设要求

一、系统要求

作为国家密钥管理系统业务功能的延伸,省级密钥管理系统的设计与建设应符合如下要求:

1、应能导入国家密钥管理系统下发的省级密钥;

2、可以提供密钥生产、密钥存储、密钥分发、密钥管理等服务，具备对称密钥的生成、注入、导出、备份、恢复、更新、服务等功能;

3、应确保密钥多级管理的可操作性。密钥的装载、存放和分散必须在安全的环境下完成，中间结果不得被内部操作人员和外界获得;

4、支持通过AB码单方式，产生省级根密钥;

5、应能为用户提供各类母卡的生产服务，生成各类母卡时要求同时生成密钥母卡及传输卡;

二、运行环境

1、省级密钥管理系统应具备标准机房环境;

2、要求放置省级密钥密钥管理系统的机房配有门禁系统及 24 小时监控系统;

3、省级密钥管理系统应配有专人负责管理以及相应的管理规范。

三、验收要求

省级密钥管理系统建成后，应由省级交通主管部门组织国内密码、安全方面的专家进行现场验收。验收通过后方可投入运营。

附件二:

关于申请公路电子收费省级密钥的函

交通运输部:

按照《省级密钥管理系统建设要求》及国家行业标准要求，我省建立了公路电子收费密钥管理系统并通过验收。现申请省级密钥母卡和传输卡，请予批准。

附件：密钥管理系统验收意见。

单位（盖章）

年　月　日

附件三:

公路电子收费 PSAM 卡申请表

编号: PSAM-SQ-200X-流水号（四位）

<table>
<tr><td colspan="5">以下内容由申请人填写</td></tr>
<tr><td>单位名称</td><td colspan="4"></td></tr>
<tr><td>经办人姓名</td><td></td><td>身份证号</td><td colspan="2"></td></tr>
<tr><td>单位地址</td><td colspan="2"></td><td>邮政编码</td><td></td></tr>
<tr><td>电子邮件</td><td colspan="2"></td><td>联系电话</td><td></td></tr>
<tr><td rowspan="2">申请内容</td><td colspan="4">☐正式使用 PSAM 卡　　数量:</td></tr>
<tr><td colspan="4">☐测试用 PSAM 卡　　数量:</td></tr>
<tr><td>申请提供的证明资料</td><td colspan="4">☐身份证复印件　　☐其它（请注明）_____</td></tr>
<tr><td colspan="5">声　明
我单位申请领取 PSAM 卡，已仔细阅读并理解《申领 PSAM 卡责任书》的内容，同时承诺遵守《密钥管理规则》中之相关规定。

经办人(签名): _____　　单位公章:
_____年___月____日　　_____年____月 ___日</td></tr>
<tr><td colspan="5">以下内容由国家密钥管理承担单位填写</td></tr>
<tr><td>国家密钥管理承担单位审核意见</td><td colspan="4">☐ 同意
☐ 不同意（原因）_____
受理人（签名）:
_____年 ___月 ___日</td></tr>
<tr><td>制作情况</td><td colspan="4">制作人: _____
_____年____月 ___日</td></tr>
<tr><td colspan="5">PSAM 卡领取情况</td></tr>
<tr><td colspan="5">领取人: _____　　_____年_____月____日</td></tr>
</table>

*本申请表一式三份,申请者留存一份，国家密钥管理承担单位留存两份。

申领 PSAM 卡责任书

PSAM 卡是用于认证非现金支付 IC 卡及车载单元，以完成公路电子收费交易。为确保公路电子收费交易的安全，省级密钥管理承担单位必须遵循以下规程:

一、 PSAM 卡是公路电子收费系统的一部分，只能用于公路电子收费系统，不能作为其他任何用途。

二、应仔细阅读《密钥管理规则》，并按照安全操作流程对 PSAM 卡进行管理与使用。

三、应根据规定填写详细的 PSAM 卡的申领与使用记录。

四、应保证 PSAM 卡的安全，如有遗失，应在 2 个工作日内以书面形式上报至国家密钥管理承担单位。

五、使用过程中如有 PSAM 卡损坏，应及时提出书面申请并进行更换。

六、若发现某些 PSAM 卡可能存在安全问题，应及时向国家密钥管理承担单位和相关部门汇报，在其使用范围内，停止使用该 PSAM 卡，并进行调换。

单位（盖章）

日期: _____年____月 ___日

附件四:

公路电子收费ESAM模块申请表

编号: ESAM-SQ-200X-流水号（四位）

<table>
<tr><td colspan="5">以下内容由申请人填写</td></tr>
<tr><td>单位名称</td><td colspan="2"></td><td>营业执照号</td><td></td></tr>
<tr><td>经办人姓名</td><td></td><td>身份证号</td><td colspan="2"></td></tr>
<tr><td>单位地址</td><td colspan="2"></td><td>邮政编码</td><td></td></tr>
<tr><td>电子邮件</td><td colspan="2"></td><td>联系电话</td><td></td></tr>
<tr><td rowspan="2">申请内容</td><td colspan="4">☐ 用于试验、测试　　数量:</td></tr>
<tr><td colspan="4">☐ 用于正式生产　　数量:</td></tr>
<tr><td>申请提供的证明资料</td><td colspan="4">☐身份证　☐营业执照　☐其它（请注明）_____</td></tr>
<tr><td colspan="5">声　明
我单位申请领取ESAM模块，已仔细阅读并理解《申领ESAM模块责任书》的内容，同时承诺遵守《密钥管理规则》中之相关规定。

经办人(签名): _____　　单位公章:
_____年___月____日　　_____年____月 ___日</td></tr>
<tr><td colspan="5">以下内容由国家密钥管理承担单位填写</td></tr>
<tr><td>国家密钥管理承担单位审核意见</td><td colspan="4">☐ 同意
☐ 不同意（原因）_____
受理人（签名):
_____年 ___月 ___日</td></tr>
<tr><td>制作情况</td><td colspan="4">制作人: _____
_____年____月 ___日</td></tr>
<tr><td colspan="5">ESAM领取情况</td></tr>
<tr><td colspan="5">领取人: _____　　_____年_____月____日</td></tr>
</table>

*本申请表一式三份,申请者留存一份，国家密钥管理承担单位留存两份。

申领 ESAM 模块责任书

ESAM 模块是用于完成车载单元的认证，以安全的完成公路电子收费交易。为确保公路电子收费交易的安全，领用 ESAM 模块的单位必须遵循以下规程:

一、 ESAM 模块是公路电子收费系统的一部分，只能用于公路电子收费系统，不能作为其他任何用途。

二、应仔细阅读《密钥管理规则》，并按照安全操作流程对 ESAM 模块进行管理与使用。

三、应根据规定填写详细的 ESAM 模块的申领与使用记录。

四、应保证 ESAM 模块的安全，如有遗失，应及时通知国家密钥管理承担单位。

五、使用过程中如有 ESAM 模块损坏，应及时提出书面申请并进行更换。

六、若发现某些 ESAM 模块可能存在安全问题，应及时向国家密钥管理承担单位和相关部门汇报。

单位（盖章）

日期: _____年____月 ___日