

居民健康卡密钥管理办法

V1.0

2011 年 11 月

第一章 总 则

第一条 为了加强卫生部居民健康卡密钥的安全管理,规范密钥管理工作操作流程,确保卫生系统各级密钥管理部门各项工作安全、有序开展,特制订此管理办法。

第二条 居民健康卡密钥管理采用两级密钥管理体制:全国密钥管理和省(直辖市)级密钥管理。

第三条 由卫生部设立部级密钥管理中心(一级密钥管理中心),该中心隶属于部居民健康卡管理中心。各省(直辖市、自治区)卫生厅设立省市级密钥管理中心(二级密钥管理中心),该中心隶属于省居民健康卡管理中心。

第四条 卫生部负责制定全国密钥管理的总体规划,负责部级、省市级密钥管理中心的业务督导和业务培训,负责“部级密钥管理系统”的日常运行和维护。

第五条 各省卫生厅负责制定本省密钥管理规划,负责本省密钥管理系统的日常运行和维护。

第二章 密钥类型

第六条 居民健康卡系统使用的密钥有以下几种类型:

(一) 非对称密钥,包括卫生部一级根密钥,发卡机构二级根密钥,SAM卡签名密钥。

(二) 卡片管理类密钥,包括居民健康卡主控密钥、居民健康卡维护密钥、SAM卡主控密钥、SAM卡维护密钥。

(三) 应用管理类密钥,包括居民健康卡全国应用主控密钥、居民健康卡全国应用维护密钥。

第七条 非对称密钥采用两级管理架构，部级密钥管理中心自签“根公钥证书”，并为发卡机构签发“发卡机构公钥证书”，发卡机构签发终端 SAM 卡公钥证书。

第八条 对称密钥采用两级建设三级分散机制生成。两级建设是指对称密钥需要建设部级密钥管理中心和省市级密钥管理中心。部级密钥管理中心生成根密钥，通过分散机制逐级下发至省市级密钥管理中心，直至居民健康卡和终端 SAM 卡。

第九条 为支持跨区域使用，SAM 卡必须装载全国应用根密钥，全国应用根密钥经过二次分散后加载到居民健康卡中，一级分散因子通过省代码生成，二级分散因子通过居民健康卡序列号生成。

第十条 为了降低密钥泄漏的风险，密钥管理系统应保证密钥的装载、存放和分散必须在安全的环境下完成，保证任何中间结果不被内部操作人员和外界获得。

第三章 部级密钥管理工作

第十一条 卫生部全国密钥管理中心负责生成和管理居民健康卡一级非对称根密钥和一级对称根密钥。

第十二条 卫生部全国密钥管理中心负责自签根公钥证书，负责签发发卡机构公钥证书，并负责为全国医疗机构、结算机构和居民健康卡管理机构签发 SAM 卡公钥证书。

第十三条 卫生部全国密钥管理中心负责分散生成省市级根密钥，采用安全的方式下发到省市级密钥管理中心。

第十四条 卫生部全国密钥管理中心负责部居民健康卡管理中心密钥管理系统运行、日常维护工作。

第十五条 卫生部全国密钥管理中心负责各类根密钥的安全保

管工作。

第四章 省市级密钥管理工作内容

第十六条 省市级密钥管理中心负责向部居民健康卡管理中心申请和接收省市级根密钥和全国共享应用密钥。

第十七条 省市级密钥管理中心采用批量方式向卫生部申请发放 SAM 卡，并负责本省 SAM 卡的安全分发和安全管理。

第十八条 省市级密钥管理中心负责为居民健康卡个人化提供下级根密钥发放服务。

第十九条 省市级密钥管理中心负责本省密钥管理系统的运行、维护工作

第二十条 省市级密钥管理中心负责卫生部下发的密钥卡片、设备以及省市级密钥管理相关的密钥、设备的安全保管工作。

第五章 人员组成和职责

第二十一条 全国密钥管理中心人员组成：密钥主管（一人）、密钥管理员（三人），密钥保管员（一人）。

第二十二条 各省市级密钥管理中心人员组成：密钥主管（一人）、密钥管理员（二人），密钥保管员（一人）。

第二十三条 密钥主管的主要工作是负责密钥管理中心的日常运行管理，密钥管理工作规划和业务需求，应急措施和备用机制建立。

第二十四条 密钥管理员的主要职责是进行日常系统运行维护、密钥管理和发卡操作，并保存日常使用到的密钥（卡）和设备。

第二十五条 条密钥保管员负责封存非日常使用的密钥（卡）和

密码。

第二十六条 为保障系统安全性，部居民健康卡管理中心和省居民健康卡管理中心使用专用保险箱妥善保管敏感信息和核心设备，针对密钥管理中心启用、恢复、省市级密钥卡申领、SAM 卡发卡、卡片采购以及库存管理等日常工作制定相应的工作流程，严格按照工作流程开展工作，并接受上级部门的监督和检查。

第六章 部级根密钥管理业务流程

第二十七条 部级根密钥管理系统负责产生非对称根密钥、卡片总控密钥和用于跨省交易的全国应用根密钥；为各省、直辖市二级密钥管理系统分散产生对应省市级根密钥，签发发卡机构公钥证书。

第二十八条 由对称密钥管理系统生成相应的对称密钥。通过领导按下选择按钮后经密码机产生随机种子密钥并存在领导卡(CPU 卡)中，领导卡通过 PIN 码保护，对称密钥管理系统通过多张领导卡同时在线，验证领导卡 PIN 码正确后读出领导卡中的随机种子密钥，送入密钥管理系统加密机经过相应算法，生成所有的密钥。

第二十九条 由根证书管理系统密码机生成非对称根密钥，并自签根公钥证书。采用 (5, 3) 门限方案将非对称根密钥备份到 5 张密钥备份卡，分存于卫生部 5 个不同的部门。以便在必要时，任选其中 3 张密钥备份卡，可恢复全部系统根密钥。

第三十条 卫生部根密钥管理系统向省市级密钥管理系统传输分散后的省市级根密钥时，可选用两种模式中的一种：一种是通过在线的方式，采用加密机对加密机的安全传输方式将上级密钥下发到下级密钥管理中心的密码机中。另一种方式是采用密钥母卡传递的方式，由上级密管中心生成密钥母卡和认证卡，然后通过人工申领的方式

式，并要求必须两人领取，每人分别保管其中的一张卡，以加强传递中的安全性。

第七章 省市级密钥管理业务流程

第三十一条 省市级密钥管理中心负责向卫生部全国密钥管理中心申请使用和接收省市级根密钥，为下级单位分散生成下级根密钥。

第三十二条 为确保系统安全性，避免密钥泄漏，省市密钥管理部门应先向部居民健康卡管理中心密钥管理部门申请省市级密钥管理测试密钥，以便进行系统测试，成功接收测试密钥后，再申请省市级正式密钥。

第三十三条 省市级密钥管理部门向部居民健康卡管理中心密钥管理部门申请测试、正式省市级密钥均需提交《卫生部省市级密钥申请表》。同时在本省市级密钥管理中心密码机中生成公私钥对，生成并提交自签名的公钥输出文件。

第三十四条 部级居民健康卡管理中心密钥管理部门在接收申请表后的二个工作日内，以《卫生部省市级密钥申请表-回复》形式进行回复，回复信息中包含密钥领取时间，测试密钥领取时间不晚于申请表接收时间的三个工作日内，正式密钥领取时间不晚于申请表接收时间的五个工作日内。

第三十五条 部级居民健康卡管理中心密钥管理部门接收到省市级密钥管理部门申请后，由密钥管理员为省市级密码机签发设备公钥证书、并以公钥加密的方式导出省市级根密钥，制作省市级密钥母卡。

第三十六条 密钥母卡制作完毕后，部级居民健康卡管理中心密

钥管理部门通知申请省密钥管理中心领卡，测试卡可以通过邮寄方式寄送到省密钥管理部门，正式卡采用省卫生厅到部级居民健康卡管理中心密钥管理部门现场领卡方式，领卡人员为申请表上的卡片接收人，领卡人员至少二人。

第三十七条 现场领卡时由省卫生厅领卡人员和部级居民健康卡管理中心密钥管理部门密钥管理人员进行交接，登记卡片交接记录，同时告知领卡人员卡片密码，测试卡密码以口头或电子邮件方式通知省中心。

第三十八条 省市级密钥管理中心将全国密钥管理中心下发的二级根密钥导入本地密码机中。

第三十九条 密钥母卡由省市级密钥管理中心密钥保管员安全保管。

第四十条 省市级密钥管理中心可参照本办法为下级发卡单位按对称密钥分散机制制作发卡母卡，具体办法由省卫生厅制定，并报卫生部审核备案。

第八章 SAM 卡发卡业务流程

第四十一条 SAM 卡由卫生部全国密钥管理中心统一签发 SAM 卡公钥证书、装载全国应用根密钥、并装载其它密钥和管理信息。

第四十二条 各省市级密钥管理中心向全国密钥管理中心批量申领 SAM 卡。

第四十三条 省市级密钥管理中心填写《卫生部 SAM 卡申请表》，加盖省市级密钥管理部门公章，并将 SAM 卡申请表寄送到部居民健康卡管理中心全国密钥管理中心。同时需要提供详细的 SAM 卡制卡电子数据，电子数据应进行加密处理。

第四十四条 卫生部全国密钥管理中心接收到省卫生厅 SAM 卡发卡申请后，密钥主管在五个工作日内针对申请和电子数据进行审核并回复，回复内容包括领卡时间。

第四十五条 卫生部全国密钥管理中心进行 SAM 卡制卡。SAM 卡生成非对称公私钥对(在卡内生成)，签发 SAM 卡公钥证书，将 SAM 卡公钥证书和发卡机构证书写入 SAM 卡，在卡片上记录 SAM 卡序列号、装载全国应用根密钥、并根据 SAM 卡用途装载其它对称密钥。

第四十六条 SAM 卡制卡完毕后，卫生部居民健康卡管理中心密钥管理部门通知申请省密钥管理中心领卡。领卡时由省密钥管理中心领卡人员和部居民健康卡管理中心密钥管理中心密钥管理人员进行交接，登记卡片交接记录。

第四十七条 省卫生厅应根据本省情况制定 SAM 卡分发、使用等具体管理办法，由省市级密钥管理中心执行。

第四十八条 省市级密钥管理中心对 SAM 卡操作过程中损坏的 SAM 卡应如数及时退回一级密钥管理中心统一销毁，并对其原来的登记情况给予注销。

第四十九条 省市级密钥管理中心将挂失、注销的 SAM 卡即时上报卫生部密钥管理中心，上报时应包括 SAM 卡卡号和挂失、注销时间等基本信息。卫生部密钥管理中心将已挂失、注销的 SAM 卡记入 SAM 卡黑名单。

第五十条 卫生部密钥管理中心每周定期生成和发布 SAM 卡黑名单。

第九章 硬件密码机管理

第五十一条 硬件密码机是进行密钥生成、存储和密码运算的安

全设备，部署在各级密钥管理系统和制卡系统机房，其网络以及硬件维护工作由相关应用系统维护人员完成，密钥注入和管理由密钥管理人员完成。

第五十二条 密码机必须部署在具有屏蔽措施的机房，并置于24小时监控之下。

第十章 附 则

第五十三条 本办法由中华人民共和国卫生部负责解释。

第五十四条 本办法自发布之日起施行。