**浙江公司物联网卡制卡管理办法**

**（2024版）**

**中国移动通信集团浙江有限公司**

**二○二四年六月**

# 

**目录**

[第一章 总则 1](#_Toc4315)

[第二章 组织管理 1](#_Toc9047)

[第三章 物联网卡定义 2](#_Toc19210)

[第四章 密钥管理 3](#_Toc16807)

[第五章 数据管理 5](#_Toc13091)

[第六章 采购及库存管理 7](#_Toc17258)

[第七章 生产管理 8](#_Toc30289)

[第八章 物联网卡质量管理 10](#_Toc15510)

[第九章 卡商管理 11](#_Toc28234)

[第十章 监督检查与问责 12](#_Toc10069)

[第十一章 附则 13](#_Toc16050)

# 总则

**第一条** 目的

为规范全省物联网卡管理，明确物联网卡制卡生产管理流程和职责分工，建立风险防范机制，省公司政企客户部依据集团公司相关规定制订本办法。

**第二条** 内容

本办法对物联网卡制卡流程的组织管理、物联网卡定义、密钥管理、数据管理、采购管理、生产管理、库存管理、物联网卡质量管理、人员管理、卡商管理、卡版面管理等进行明确，是全省进行物联网卡制卡生产和管理的基本依据。

**第三条** 适用范围

本办法适用于省公司和各市分公司。

# 组织管理

**第四条** 分级管理

总部负责全国物联网卡制卡的整体管理工作，省公司负责省内物联网卡制卡的管理工作，地市公司负责本地市的制卡管理工作。

**第五条** 省公司职责

省公司负责全省物联网卡需求审批、需求上报、制卡申请、订单制作、省本级集中备卡仓储库存和出入库等管理。

**第六条** 地市公司职责

市分公司负责本地市物联网卡制卡需求报送及本地卡品仓储库存及出入库管理，负责本地市的物联网卡库存的呆滞物资和“两金压降”管理工作。

**第七条** 物联网卡制卡系统运营单位

信息技术中心、物联网公司、省公司网络部门及IT部门为物联网卡制卡的配合单位和系统运营单位（以下统称各系统运营单位）。各系统运营单位根据物联网卡密钥和数据管理工作需要，配置必要的监督和操作人员，完善岗位职责设置，其中密钥管理人员和卡数据管理人员岗位应分开设置，避免密钥和卡数据由同一人掌握，配合总部制定涉卡人员清单并按总部要求定期更新。

# 物联网卡定义

**第八条** 物联网卡定义

物联网卡是应用于物联网领域的SIM卡，要求采用物联网专用号码作为通信号码，承载于物联网核心网专用网元。

**第九条** 主要功能

物联网卡主要功能是提供登网鉴权、存储安全数据、提供安全运算能力等。

**第十条** 物联网卡分类

（一）按照卡的技术类型分为普通物联网卡、eSIM卡等。普通物联网卡是指可用于2/3/4/5G、NB-IoT网络下，为终端提供登网鉴权能力的单一功能物联网卡。eSIM卡是指支持切换profile的物联网卡，目前支持的范围参见《工信部信管函[2020]225号》。

（二）普通物联网卡按照卡内数据存储情况分为实卡、临时号卡和预置空白卡。实卡指包含了K（鉴权密钥）\OPc（每卡唯一的算法配置变量）\IMSI（国际移动用户识别码）\ICCID（集成电路卡识别码）\SMSP（短消息中心）五码数据的物联网卡；临时号卡指包含临时五码数据的物联网卡，该卡在正式使用时写入正式五码数据；预置空白卡指不包含五码数据的物联网卡，该卡在使用时写入五码数据。

（三）eSIM卡按照卡内数据存储情况分为预置profile、不预置profile。预置profile的eSIM卡指制卡时写入profile的eSIM卡；不预置profile的eSIM卡指制卡时不写入profile，该卡在使用时写入profile。

**第十一条** ICCID编码管理

具体要求参见《中国移动ICCID编码规则》。

# 密钥管理

**第十二条** 密钥的作用与分类

本办法中的“密钥”是指对物联网卡数据进行加密、解密、数据完整性保护等操作所使用机密参数，用于保证数据在传输、存储等过程中的安全性。根据密钥的用途可以将密钥分为存储密钥、传输密钥和写卡密钥，其中存储密钥用于各系统保护本地存储的物联网卡数据，传输密钥用于各系统间传递物联网卡数据过程中提供保护，写卡密钥包括普通物联网卡写卡密钥和eSIM卡写卡密钥，分别用于专网写卡平台和onelink 5G智能网联管理平台在写卡过程提供数据保护。

**第十三条** 密钥安全管理

密钥管理操作包括生成、传输、更新、备份、销毁等环节，每一类操作均应保证双人控制，确保密钥生命周期安全。其中，密钥应由加密设备随机生成，并安全保存在加密设备内；除公钥之外的密钥应采用IC卡进行安全传输；对于需要更新的密钥，应按照密钥生成的要求，重新生成。

备份密钥应存储在IC卡中或者专用的备份系统中，其中IC卡介质应由系统所属运营单位负责保管，并设置专用保险柜，由双人控制；备份在系统中的密钥由系统所属运营单位负责管理；不再使用的密钥应进行安全销毁。

**第十四条** 密钥有效期要求

存储密钥和普通物联网卡写卡密钥（根密钥）有效期最长为5年，eSIM卡写卡密钥（SM-DP+证书）有效期最长为3年，传输密钥有效期最长为2年。各系统运营单位应根据所管理密钥的有效期要求，确保在有效期满之前完成相应密钥更新工作。如密钥更新涉及多系统协同配合，系统运营单位可向总部政企事业部申请，由总部政企事业部协同组织各系统运营单位评审和实施。如有特殊情况需延长有效期，系统运营单位应向总部政企事业部申请评估，由总部政企事业部协同总部网络事业部、信安中心、研究院、信息技术中心及物联网公司等单位组建专家团队进行评估，确认风险可控，方可进行延期。密钥有效期内如存在安全隐患，系统运营单位应及时组织开展密钥更换工作。

**第十五条** 密钥算法要求

各系统运营单位须采用足够安全强度的标准算法，并优先采用国密算法，保证在密钥生命周期内不被破解。

# 数据管理

**第十六条** 物联网卡数据分类

物联网卡数据分为电信数据和非电信数据，电信数据指写入电信应用的各项个人化数据，包括K、OPc、IMSI、ICCID、PIN、PUK等。非电信数据指写入非电信的各项个人化数据，包括卡标识、写卡密钥等。

**第十七条** 物联网卡数据安全管理原则

物联网卡数据管理涉及数据生成、存储、传输、写入、回收等，各系统运营单位应依据本办法，制定或完善各系统及数据管理人员的卡数据保密管理要求。禁止将涉及物联网卡数据生成、加解密的系统以任何形式连接到外部互联网。卡数据仅能提供给中国移动的物联网卡供卡商，卡商范围详见《ICCID卡商编码表》。

**第十八条** 物联网卡数据系统管理

目前物联网卡涉及系统有移动侧的物联网集中化支撑系统(CMIOT)、鉴权数据中心（UDM）、物联网写卡服务平台（专网写卡平台、onelink 5G智能网联管理平台等），以及卡商侧的制卡系统，各系统应配备必要的加密设备，并做好账号访问控制、日志管理等安全管理，具体要求参见《中国移动 IT 领域数据安全管理办法》、《中国移动通信集团有限公司数据安全管理办法（试行）》及信安、IT与网络侧下发的相关安全管理要求。

**第十九条** 数据生成管理

省公司在物联网集中化支撑系统（CMIOT）上发起制卡申请，经由集团公司侧后端对接系统（包含写卡平台等）生成对应的卡数据信息，仅集团公司侧经授权的卡号管理人员进行数据生成操作，且数据生成前应有身份认证、权限验证环节。

**第二十条** 数据存储管理

卡数据在物联网集中化支撑系统(CMIOT)、UDM、物联网写卡服务平台以及卡商制卡系统内遵循最小化存储原则，使用各自的存储密钥加密存储，其中在卡商制卡系统内存储时间不超过12个月且须有详细的存储记录备查。

**第二十一条** 数据传输管理

卡数据传输过程必须对敏感数据（包括K、OPc等）进行加密，并使用安全的传输方式。数据传输使用的算法应具备标识能力，可分环节追溯。与卡商之间的数据传输进行全量数据加密及数字签名，并建立安全可靠的传递机制。

**第二十二条** 数据写入管理

物联网卡数据写卡主要有厂商工厂内写入和远程写卡两种方式。厂商工厂内写入要求在安全认证的环境内写入，数据应在工厂独立数据室接收及处理；远程写卡指卡片出厂时并无正式码号数据，通过读卡器、授权APP或空中等方式完成正式码号数据的写入、更新，远程写卡过程应保证数据加密、通信安全、流程安全。

写卡时对用户敏感信息进行终端查询、展现、统计等操作时，如果展示对象不是客户本人，应按照最少够用原则，严格实施脱敏处理，对于未经脱敏处理的，必须纳入金库模式管控。其他用户实名信息管理要求参见《电话用户真实身份信息登记实施规范》及监管上级部门其他管理要求。

**第二十三条** 数据回收

物联网集中化支撑系统（CMIOT）应具备可回收的IMSI资源的能力，实现资源的回收利用，确保IMSI的可用量，避免IMSI资源枯竭。

# 采购及库存管理

**第二十四条** 物联网卡采购应遵循满足市场需求和总量控制的原则，应有效保证物联网卡供应，同时合理控制采购成本。

**第二十五条** 列入总部一级集中采购目录的物联网卡，由总部政企事业部收集省公司采购需求。地市分公司按需向省公司报送制卡需求，省公司有效评估实际需求上报总部政企事业部，由总部政企事业部委托供应链管理中心执行采购。省公司按照总部下发的集采结果及本省集采份额制作订单。

**第二十六条** 对于一级集中采购目录外的特殊卡品，省公司和市公司可按照供应链管理部相关规范组织采购。

**第二十七条** 物联网卡的保管应设置安全的存储环境，各市公司应设置物联网卡专用出入库管理台帐，做到账务与卡实物管理职责与管理人员分离，建立物联网卡定期盘存管理制度，做好盘点记录，建立物联网卡稽核流程。物联网卡使用应做到先进先出，降低滞库时间，由于技术更新、业务下线、实物损坏导致的废卡由省专公司进行报废处理。具体实施依据《中国移动物流管理办法》、《中国移动物流管理实施细则》、《中国移动存货管理办法》。

# 生产管理

**第二十八条** 物联网卡及卡数据生产的原则

市公司应根据市场需求，合理制定生产数量。为加强物联网卡生产的严肃性，应制定科学合理的分级审批流程。物联网卡生产须由专人负责，配备专用终端，并安装主机防护软件，开启水印等防护策略，在安全的环境下进行相关操作，确保物联网卡生产安全。

**第二十九条** 卡数据生产流程

（一）普通物联网卡数据生产

普通物联网卡生产需求须经市分公司政企部审核，经省公司政企部审批，审批通过后由省公司政企部向物联网集中化支撑系统(CMIOT)发起制卡请求，物联网集中化支撑系统(CMIOT)生成卡数据（K\OPc\IMSI\ICCID\SMSP等），写卡服务平台生成KIC,KIK等信息，由物联网集中化支撑系统(CMIOT)按规则完成加密后传输给集团公司卡数据统一下载中心。

（二）eSIM卡数据生产

eSIM卡生产需求须经市分公司政企部审核，经省公司政企部审批，审批通过后由省公司政企部向物联网集中化支撑系统(CMIOT)发起制卡请求，物联网集中化支撑系统(CMIOT)生成卡数据（K\OPc\IMSI\ICCID\SMSP等），并完成加密后传输给物联网公司。

**第三十条** 物联网卡的生产流程

（一）普通物联网卡生产流程

1、市分公司政企部向省公司政企部提交制卡需求工单；

2、省公司政企部对市分公司的制卡需求单进行审批；

3、省公司政企部对于审批通过的需求单，在CMIOT系统发起制卡申请，集团公司侧后端对接系统（包含写卡平台等）生成对应的卡数据，省公司政企部在供应链系统制作制卡订单；

4、卡商收到制卡订单后，在集团公司统一下载中心下载卡数据，卡商下载数据后进行实物卡制作；

5、制作完成后通过专属物流邮寄给省公司，在省公司集中备卡中心完成卡片实物入库；

6、市分公司向省公司发起备卡申请，省公司将卡品实物调拨到市分公司仓库。

（二）eSIM卡生产流程

对于有实体卡制卡需求的eSIM，制卡流程同物联网卡生产；对于没有实体卡制卡需求的eSIM，无制作实体卡流程，由用户通过终端设备向物联网公司发起写卡请求或由onelink 5G智能网联管理平台主动下发写卡指令，通过onelink 5G智能网联管理平台将卡数据下载并写入设备的eSIM卡上。

**第三十一条** 卡版面管理

一级集中采购目录的物联网卡的基础版面由集团公司统一设计，具体依照《中国移动USIM卡卡体及包装规范》。省市公司可结合本地客户需求，适度调整物联网卡卡体及包装，如卡体颜色、卡基版面设计等，但不可向卡体或卡基喷刷未经集团公司和省公司授权的含有链接信息的二维码或条形码等。

# 质量管理

**第三十二条** 物联网卡质量管理主要包括物联网卡质量标准的制定、质量检测、监督检查和结果处理等的管理。

**第三十三条** 物联网卡质量标准的制定

1. 对于集团公司集采的物联网卡，由集团公司确定总体业务与技术要求并制定物联网卡质量管理规范。

（三）对于非集团公司集采的物联网卡，省公司和市分公司可自行制定质量规范。

**第三十四条** 物联网卡质量检测和监督检查

（一）供应链管理中心牵头，研究院配合完成物联网卡产品的标准符合性检测。

（二）供应链管理中心负责针对市场上各物联网卡供应商的卡产品进行质量抽查。

（三）省公司在研究院卡测试管理平台执行物联网卡到货抽检，并完成业务功能测试等工作。供应链管理中心定期对到货检测执行情况进行抽查，并对抽查结果进行通报。

（四）市分公司负责分析和记录客户对物联网卡质量问题的投诉，并定期上报省公司，省公司汇总质量问题并向相关部门上报。

**第三十五条** 物联网卡质量跟踪处理

供应链管理中心牵头，研究院配合，根据抽查结果以及省公司反馈的质量问题，对各卡供应商进行质量跟踪及问题处理。

# 卡商管理

**第三十六条** 中国移动物联网卡卡商定义

通过资质审核并获得中国移动卡商编码的物联网卡供应商为中国移动物联网卡卡商（简称卡商）。集团公司与卡商签订集采合同，统一对卡商进行管理。

**第三十七条** 准入与退出要求

卡商须具备独立安全的场地和相关安全生产资质，具体准入以及退出要求由政企事业部通过《中国移动物联网USIM卡产品集中采购总体业务与技术要求》明确并定期更新，供应链管理中心按照政企事业部要求与采购相关管理要求进行卡商的集采与负面行为处理、后评估等。

**第三十八条** 管理要求

省公司依照《中国移动物联网USIM卡产品集中采购总体业务与技术要求》，与卡商签订安全保密协议，确保卡商数据安全与供卡质量。卡商如有供卡质量等问题，依照《中国移动一级集中采购供应商负面行为处理规则》执行。

**第三十九条** 因物联网车联网业务发展需求，如车企客户提出指定制卡卡商未中标当期物联网卡一级集采框架，则须遵照《中国移动车企客户自采物联网卡业务模式操作流程（2024版）》相关要求执行申请、审批、报备等管理流程,具体流程参见附件1。

**第四十条** 总部政企事业部及供应链管理中心牵头每年组织一次卡商抽检，对卡商的资质、人员管理、数据安全管理等方面进行检查，并进行记录。卡商由总部统一管理，省公司每年配合总部在供应链系统对卡商服务情况进行考核打分，卡商如有发生严重质量事故或数据安全事故的，省公司可在卡商年度考核评分中进行扣分，考核评分由省供应链管理部提交至总部，总部根据省公司提供的评分，依据集采合同对卡商进行考核管理。

**第四十一条** 卡商须按照总部规定建立涉卡数据人员清单，配置必要的监督和操作人员，完善岗位职责设置，其中密钥管理人员和卡数据管理人员岗位应分开设置，避免密钥和卡数据由同一人掌握，并按照实际情况进行更新以备检查，且须对清单内人员定期开展安全警示教育与培训，提升员工安全意识。卡商在制卡过程中须严格保障卡数据安全，具体依照《中国移动物联网USIM卡产品集中采购总体业务与技术要求》。

# 监督检查与问责

**第四十二条** 省公司政企部门按照上级要求，牵头开展本省的物联网卡监督检查，每年开展常态化自查，建立业务检查清单与安全检查清单，对检查发现的问题严格追责并进行整改。

**第四十三条** 问责管理

（一）违反本办法，有下列情形之一并对公司造成重大损失的，应对相关责任人给予相应处罚：

1、未按管理办法规定，违反业务相关管理和审批流程；

2、参与或因疏于监管导致卡数据或密钥丢失、泄露等造成不良影响。

（二）省公司政企部对省内制卡规范执行情况每年开展自查，对于违反本管理办法中各项管理规定，将予以通报，尤其是违反卡数据安全要求的，必须限期整改并进行问责。

（三）凡违反本办法规定，给公司造成经济损失和重大影响的，依据《中国共产党纪律处分条例》、《中共中国移动通信集团公司党组问责工作管理办法》、《中国移动通信集团公司员工违纪违规处分条例（试行）》、《中国移动通信集团公司经理人问责实施办法（试行）》及《中国移动网络安全工作考核问责办法》等相关规定，追究有关人员的责任。

# 附则

**第四十四条** 本办法由中国移动浙江公司政企客户部负责解释。各市分公司可在本管理办法基础上根据实际情况，制定本地的实施细则。

**第四十五条** 本办法自发布之日起实施。