ICS 35.020
CCS L 70

团　　体　　标　　准

T/CERS 0004—2023

电力移动互联网应用个人信息及接口安全防护技术要求

Technical requirements for personal information and interface security protection of power mobile internet applications

2023－12－25 发布　　2023－12－25 实施

中　国　能　源　研　究　会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本文件由中国能源研究会归口。

本文件起草单位：国网智能电网研究院有限公司、上海上讯信息技术有限公司、国家电网公司客户服务中心、国网数字科技控股有限公司、国网重庆市电力公司、国网湖南省电力有限公司、国网江苏省电力有限公司。

本文件主要起草人：李勇、陈璐、卢子昂、陈牧、张涛、马媛媛、李尼格、邵志鹏、戴造建、方文高、王腾岩、陆晓雄、王晨飞、彭轼、靳敏、陈中伟、夏飞、李树、赵新建、石琳珊。

本文件首次发布。

本文件在执行过程中的意见或建议反馈至中国能源研究会。

相关意见反馈联系方式：中国能源研究会标准执行办公室（E-mail: cers@cers.org.cn；Tel：010-56284696）、中国能源研究会信息通信专业委员会标准工作委员会（E-mail:icc@cers.org.cn）。

电力移动互联网应用个人信息及接口安全防护技术要求

1 范围

本文件规定了电力移动互联网应用个人信息及接口安全防护技术要求，包括电力移动互联网应用个人信息和接口类型、个人信息保护要求及接口安全防护要求。

本文件适用电力移动互联网应用的技术评估、监督检查和安全防护。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB 17859 计算机信息系统安全保护等级划分准则

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 25069 信息安全技术 术语

GB/T 32905 信息安全技术 SM3密码杂凑算法

GB/T 32907 信息安全技术 SM4分组密码算法

GB/T 35273 信息安全技术 个人信息安全规范

GB/T 35276 信息安全技术 SM2密码算法使用规范

GB/T 35278 信息安全技术 移动终端安全保护技术要求

GB/T 37964 信息安全技术 个人信息去标识化指南

GB/T 38636 信息安全技术 传输层密码协议(TLCP)

GB/T 41391 信息安全技术 移动互联网应用程序（App）收集个人信息基本要求

电力行业网络安全等级保护管理办法 国能发安全规〔2022〕101 号

3 术语和定义

GB/T 22239、GB/T 25069、GB/T 35273和GB/T 35278界定的以及下列术语和定义适用于本文件。

3.1

电力移动互联网应用 power mobile internet application

电力企业开展业务服务基于移动操作系统开发的互联网应用软件。

注：简称电力移动App。

3.2

电力移动互联网应用接口 power mobile application interface

电力移动互联网应用对外提供功能访问的通道，外部开发者可以通过访问该通道获取电力企业应用服务，无需关注服务具体设计与实现。

3.3

逻辑隔离 logical isolation

指处于不同安全域的网络在物理上是有连线的，通过协议转换的手段保证受保护信息在逻辑上是隔离的，只有被系统要求传输的、内容受限的信息可以通过。

3.4

数据脱敏 data masking

一种数据保护技术，通过对原始数据进行变换、替换、混淆等方式，将敏感信息部分或全部隐藏，达到数据保密的目的。

3.5

数字水印 digital watermark

通过特定算法将特定信息嵌入到多媒体内容中以实现文件真伪鉴别、版权保护等功能的数据保护技术。

3.6

去标识化 de-identification

通过对个人信息的技术处理，使其在不借助额外信息的情况下，无法识别或者关联个人信息主体的过程。

4 缩略语

下列缩略语适用于本文件：

App：应用程序（Application）

API：应用程序接口（Application Programming Interface）

IMEI：国际移动设备识别码（International Mobile Equipment Identity）

IMSI：国际移动用户识别码（International Mobile Subscriber Identity）

MAC：介质访问控制（Medium Access Control）

REST：表述性状态传递（Representational State Transfer）

SDK：软件开发工具包（Software Development Kit）

SOAP：简单对象访问协议（Simple Object Access Protocol）

SQL：结构化查询语言（Structured Query Language）

SSL：安全套接层（Secure Sockets Layer）

TLS：安全传输层协议（Transport Layer Security）

5 总体要求

5.1 电力移动 App 个人信息安全要求应按照 GB/T 35273 的规定，满足“权责一致、目的明确、选择同意、最小必要、公开透明、确保安全、主体参与”基本原则。

5.2 电力移动 App 接口安全防护应按照 GB 17859 的规定，划分系统安全定级后，按照 GB/T 22239 和《电力行业网络安全等级保护管理办法》的规定进行防护。

6 电力移动互联网应用个人信息和接口类型

6.1 个人信息类型

电力移动App所涉个人信息类型包括电力用户身份和鉴权信息、电力用户服务信息、电力用户服务依赖信息三类。

a) 电力用户身份和鉴权信息是用于电力移动App对用户身份进行识别和鉴权的相关信息，包括电力用户身份和电力用户鉴权信息两个子类。

电力用户身份信息包括但不限于：

1） 用户基本资料：姓名、证件类型及号码、年龄、性别、地址等；

2） 身份证明：身份证、驾驶证、户口本、护照和社保卡等身份证件影印件；

3） 生物标识：指纹、人脸、虹膜等。

电力用户鉴权信息包括但不限于：

1） 电力服务鉴权信息：用电户号、客户名称、客户编号、用电地址等；

2） 普通鉴权信息：电话号码、账户、邮箱地址、个人数字证书以及服务涉及的密码和口令等。

b) 电力用户服务信息是电力移动App在提供服务过程中收集的具有隐私属性的数据，包括但不限于：

1） 服务内容信息：用电负荷、电费账单、交费记录等和电力服务相关的信息；

2） 服务日志信息：浏览记录、搜索查询记录、交易操作记录、IP地址、访问日期和时间等。

c) 电力用户服务依赖信息是电力移动App在提供服务过程中收集用于辅助开展业务相关的具有隐私属性的数据，包括但不限于：

1） 设备信息：硬件型号、IMEI号、设备MAC地址、IMSI信息等；

2） 位置信息：用户地址名称、所在经纬度、地区代码、小区代码等；

3） 金融信息：银行账户、增值税号、增值税名、产权信息、征信信息、企业营业执照等。

6.2 接口类型

电力企业依托API、SDK技术构建移动互联网应用的对外服务接口，并通过应用接口输出电力自身服务能力。

电力移动互联网应用接口按照集成方式，主要包括两种形式：

a) API接口，通过REST、SOAP等协议构建的可以直接远程调用的网络服务接口；

b) SDK接口，通过集成SDK（已封装API接口）实现本地函数级调用的服务接口。

7 个人信息保护要求

7.1 个人信息收集

电力移动App个人信息收集应在满足GB/T 41391要求的基础上，符合以下要求：

a) 电力移动App收集的个人信息应根据服务需要，原则上可采集信息包括电力用户身份和鉴权信息、电力用户服务信息、电力用户服务依赖信息三类，不得超范围收集个人信息；

b) 电力移动App收集个人信息应遵循最小必要原则，收集个人信息的数量、频次、精度等应为电力服务所必需；

c) 电力移动App收集个人信息应遵循授权同意原则，应向个人信息主体告知收集、使用个人信息的目的、方式和范围等规则，并获得个人信息主体的授权同意，不应在征得个人信息主体授权同意前，产生个人信息收集行为；

d) 电力移动App应制定个人隐私政策，其要求包括但不限于：

1） 首次运行时应通过弹窗等明显方式提示用户阅读隐私政策；

2） 应采取非默认勾选的方式征得用户同意；

3） 应向用户告知涵盖个人信息处理主体、处理目的、处理方式、处理类型、保存期限等内容的个人信息处理规则；

4） 应明示嵌入的第三方SDK名称、包名、SDK运营者名称、嵌入目的、收集的个人信息类型、使用的敏感系统权限。

7.2 个人信息传输

电力移动App个人信息传输应按照GB/T 35276、GB/T 32905、GB/T 32907等要求采用加密技术手段，防止传输过程中的个人信息泄露、窃取和篡改等安全风险。

7.3 个人信息存储

电力移动App个人信息存储要求包括：

a) 电力移动App个人信息存储期限应为实现个人信息主体授权使用的目的所必需的最短时间，超出上述个人信息存储期限后，应对个人信息进行删除或匿名化处理；

b) 电力移动App个人信息应存储在电力企业管辖范围内的平台；

c) 电力移动App应对存储的个人信息提供访问控制和加密保护；

d) 电力移动App收集的个人信息应根据GB/T 37964的要求进行去标识化处理，如采用假名、加密、哈希函数等技术手段替代对个人信息的标识；

e) 电力移动App收集的电力用户身份和鉴权信息、电力用户服务信息、电力用户服务依赖信息应采取逻辑隔离方式分开存储。

7.4 个人信息使用

电力移动App个人信息使用要求包括：

a) 对被授权访问电力移动App个人信息的人员，应建立最小授权的访问控制策略；

b) 电力移动App涉及通过界面展示个人信息的，个人信息控制者应对需展示的个人信息采取去标识化处理等措施，降低个人信息在展示环节的泄露风险；

c) 使用电力移动App个人信息时，不应超出与收集个人信息时所声称的目的具有直接或合理关联的范围。

7.5 个人信息共享、转让和公开披露

电力移动App个人信息共享、转让和公开披露要求包括：

a) 应建立个人信息共享和转让安全管理规范，确保共享和转让经过流程审核；

b) 在共享和转让前，应开展个人信息安全影响评估，并依评估结果采取有效的保护个人信息主体的措施；

c) 在共享和转让前，应开展个人信息接受方安全能力评估，并通过合同等方式规定个人信息接收方的责任和义务；

d) 应准确记录和存储个人信息的共享、转让情况，包括共享、转让的日期、规模、目的，以及数据接收方基本情况等；

e) 除法律法规规定的需提供个人信息明细数据外，应采用数据脱敏、数字水印等技术手段对共享和转让个人信息进行处理；

f) 电力移动App个人信息原则上不应公开披露，电力企业经法律授权或具备合理事由确需公开披露时，应符合以下要求：

1） 事先开展个人信息安全影响评估，并依评估结果采取有效的保护个人信息主体的措施；

2） 向个人信息主体告知公开披露个人信息的目的、类型，并事先征得个人信息主体明示同意；

3） 不应公开披露个人生物识别信息。

g) 电力移动App个人信息安全影响评估报告应至少保存三年。

7.6 个人信息主体权利

电力移动App个人信息主体权利要求包括：

a) 电力移动App运营者应向用户提供个人信息查询、更正、删除和撤回授权方法；

b) 电力移动App运营者应向用户提供注销账户的功能，注销账号的过程应简单易操作，不应设置不必要或不合理的注销条件；

c) 电力移动App运营者应建立投诉管理机制和投诉跟踪流程，并在合理的时间内对用户投诉进行及时响应，投诉到响应时间不超过15个工作日。

8 接口安全防护要求

8.1 基本安全要求

电力移动App接口基本安全要求包括：

a) 电力移动App接口使用的加解密算法、技术和产品应符合GB/T 35276、GB/T 32905和GB/T 32907等加密技术标准，符合国家密码管理部门及行业主管部门要求；

b) 应指定接口版本管理与控制规程，管理接口发布、变更、下线等全生命周期流程，规范接口版本管理；

c) 接口调用提供的异常和调试信息，不应泄露服务器、中间件、数据库等软硬件信息或内部网络信息；

d) 应定期开展接口安全评估和渗透测试，识别接口存在的安全风险和漏洞，包括但不限于越权访问漏洞、SQL注入漏洞、任意文件上传漏洞、敏感信息泄露漏洞、命令执行漏洞、关键会话重放攻击漏洞等已知安全漏洞。

8.2 身份认证

电力移动App接口身份认证要求包括：

a) 电力移动App接口应对使用者身份信息进行安全认证，对涉及企业敏感数据的关键业务接口，应采用多因子认证机制增强安全认证，包括但不限于使用静态密码、身份令牌、短信验证码、人脸识别、指纹识别等两种或两种以上组合的技术；

b) 应对接口连接时间进行限制（如接口会话或令牌有效期），避免接口连接闲置后仍长期有效。

8.3 访问控制

电力移动App接口访问控制要求包括：

a) 应按照最小授权原则，严格控制用户访问接口的资源和数据，避免超授权范围访问；

b) 应具备按需设置授权有效期或次数的功能，避免无限期授权。

8.4 传输安全

电力移动App接口传输安全要求包括：

a) 应按照GB/T 38636中传输层密码协议要求进行安全防护；

b) 应对接口通信数据进行完整性校验；

c) 应采用SSL/TLS（V1.2及以上版本）进行安全通信；

d) 对于关键业务接口，应采用数字签名、数字证书等技术手段，保证接口数据传输完整性和不可抵赖性。

8.5 集成和部署安全

电力移动App接口集成和部署安全要求包括：

a) 应提供具备接口安全开发的用户集成手册，规范接口安全使用；

b) 发布提供封装服务接口的SDK，应具备防反编译、防篡改、防调试和二次打包等安全功能；
c) 接口服务应部署在电力企业管辖范围内的平台，对涉及企业敏感数据的关键业务接口，不应托管在第三方公有云平台；
d) 接口服务应根据网络安全等级保护定级及安全要求，在互联网边界部署安全设备实现访问控制、入侵检测等安全防护能力。

8.6 风险控制

电力移动App接口风险控制要求包括：

a) 应对接口使用情况进行监控，包括调用用户、频率、时间进行定期分析统计；
b) 身份认证、资金交易等关键业务接口应识别是否经过用户本人授权，具备人机识别能力；
c) 资金交易接口应满足国家及行业监管部门对反洗钱、反欺诈等方面的相关要求；
d) 通过SDK接口访问电力服务时，SDK应具备对移动终端异常环境安全检测能力；
e) 对监控到的接口调用风险应及时处置。

8.7 安全审计

电力移动App接口安全审计要求包括：

a) 应具有安全审计功能，对接口使用情况等进行审计；
b) 接口审计日志内容应至少包括接口标识、调用对象、调用时间、返回结果等；
c) 接口审计日志留存时间不应少于180天。

参 考 文 献

[1] GB/T 37729-2019 信息技术 智能移动终端应用软件（APP）技术要求

[2] TC260-PG-20205A 网络安全标准实践指南-移动互联网应用程序（App）收集使用个人信息自评估指南

[3] TC260-PG-20205A 网络安全标准实践指南-移动互联网应用程序（App）使用软件开发工具包（SDK）安全指引

[4] 工业和信息化部关于开展纵深推进APP侵害用户权益专项整治行动的通知(工信部信管函〔2020〕164号)