团 体 标 准

移动平台客户服务管理系统设计规范

编 制 说 明

《移动平台客户服务管理系统设计规范》小组

二〇二三年四月

目　录

《移动平台客户服务管理系统设计规范》

团体标准编制说明

一、工作简况

（一）任务来源

在快速发展的时代下，移动平台应运而生，它涵盖移动应用开发、管理、安全、整合等全生命周期的统一平台。移动平台已成为企业客户服务的重要渠道，但客户服务体系搭建等机制欠缺规范，客户服务流程过于繁琐缓慢等问题，严重影响客户的使用体验。制定移动平台客户服务管理系统设计规范，使客户服务流程变得更加简单、便捷和快捷，提升客户服务质量和效率。

移动平台客户服务系统在过程中可能遇到需求不清晰、用户体验不好、流程繁琐等问题，需要进一步进行规范化设计，提升客户服务水平。现行虽有一些标准，但与目前相关行业的发展进程距离较远。因此开展移动平台客户服务管理系统设计标准研究，可以提升客户服务的质量和效率，推进企业数字化转型，增强企业竞争力，满足客户的多样化需求，并打造一个良好的客户服务体系。

（二）编制过程

为使本标准在服务管理系统设计市场管理工作中起到规范信息化管理作用，标准起草工作组力求科学性、可操作性，以科学、谨慎的态度，在对我国现有服务管理系统设计市场相关管理服务体系文件、模式基础上，经过综合分析、充分验证资料、反复讨论研究和修改，最终确定了本标准的主要内容。

标准起草工作组在标准起草期间主要开展工作情况如下：

1、项目立项及理论研究阶段

标准起草组成立伊始就对国内外服务管理系统设计相关情况进行了深入的调查研究，同时广泛搜集相关标准和国外技术资料，进行了大量的研究分析、资料查证工作，确定了服务管理系统设计市场标准化管理中现存问题，结合现有产品实际应用经验，为标准起草奠定了基础。

标准起草组进一步研究了服务管理系统设计需要具备的特殊条件，明确了技术要求和指标，为标准的具体起草指明了方向。

2、标准起草阶段

在理论研究基础上，起草组在标准编制过程中充分借鉴已有的理论研究和实践成果，基于我国市场行情，经过数次修订，形成了《移动平台客户服务管理系统设计规范》标准草案。

3、标准征求意见阶段

形成标准草案之后，起草组召开了多次专家研讨会，从标准框架、标准起草等角度广泛征求多方意见，从理论完善和实践应用多方面提升标准的适用性和实用性。经过理论研究和方法验证，起草组形成了《移动平台客户服务管理系统设计规范》（征求意见稿）。

（三）主要起草单位及起草人所做的工作

1、主要起草单位

中国中小商业企业协会、武汉掌中天下科技有限公司等多家单位的专家成立了规范起草小组，开展标准的编制工作。

经工作组的不懈努力，在 2023 年 4 月，完成了标准征求意见稿的编写工作。

2、起草人所做工作

广泛收集相关资料。在广泛调研、查阅和研究国际标准、国家标准、行业标准的基础之上，形成本标准草案稿。

二、标准编制原则和主要内容

（一）标准编制原则

本标准依据相关行业标准，标准编制遵循“前瞻性、实用性、统一性、规范性”的原则，注重标准的可操作性，本标准严格按照《标准化工作指南》和 GB/T 1.1《标准化工作导则 第一部分：标准的结构和编写》的要求进行编制。标准文本的编排采用中国标准编写模板 TCS 2009 版进行排版，确保标准文本的规范性。

（二）标准主要技术内容

本标准报批稿包括 8 个部分，主要内容如下：

1 范围

本文件规定了移动平台客户服务管理系统设计的术语和定义、基本要求、系统建设要求、系统功能要求、系统运行管理要求、系统评测与验收要求技术内容。

本文件适用于移动平台客户服务管理系统的建设。

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/T 2312 信息交换用汉字编码字符集 基本集

GB/T 2887 计算机场地通用规范

GB/T 9361 计算机场地安全要求

GB/T 9387.2 信息处理系统 开放系统互连基本参考模型 第2部分：安全体系结构

GB/T 15121.4 信息技术 计算机图形存储和传送图片描述信息的元文卷 第四部分：清晰正文编码

GB/T 15278 信息处理 数据加密 物理层互操作性要求

GB/T 17191.1 信息技术 具有1.5Mbit/s数据传输率的数字存储媒体运动图像及其伴音的编码 第1部分：系统

GB/T 17235.1 信息技术 连续色调静态图像的数字压缩及编码 第1部分：要求和指南

GB 18030 信息技术 中文编码字符集

GB 50173 电气装置安装工程66kV及以下架空电力线路施工及验收规

3 术语和定义

下列术语和定义适用于本文件。

3.1

信息服务 information service

指为了提供有效、实用、及时的信息给服务对象而制订的统一遵守的系列规则、规范。

3.2

控制目标 control target

指根据具体的计算机应用，结合实际制定出的安全控制要求。

3.3

安全漏洞 security vulnerabilities

指系统的安全薄弱环节，容易被干扰或破坏的环节和部件。

3.4

控制措施 control measures

指为实现其安全控制目标所制定的安全控制技术、配置方法及各种规范制度。

4 基本要求

4.1 一般要求

a) 系统开发应具有建设方案、安全设计方案、安全测评报告、系统服务外包协议（合同）及保密条款；
b) 应设置信息安全管理工作的职能部门，配置安全主管人、设置各方面管理岗位，明确各岗位职能与负责人员的职责；
c) 系统管理应划分不同权限，采取认证管理等安全保障措施；
d) 安全管理应符合 GB/T 9387.2、GB/T 15278 要求。

4.2 技术要求

4.2.1 物理安全

4.2.1.1 环境安全

对系统所在环境采取安全保护措施，可包括以下内容：

a) 区域保护，机房应有门禁系统、监控系统；
b) 所采取的措施应符合 GB 50173、GB/T 2887、GB/T 9361 要求。

4.2.1.2 设备安全

设备安全可包括以下内容：

a) 应具有设备的防电磁辐射与信息泄漏、抗电磁干扰；
b) 应具有电源保护与备用供电系统，系统可持续、不中断运行；
c) 设备配置应具有设备基本信息、运行维护、安全策略、备份等；
d) 应建立网络与信息系统安全应急响应管理制度等。

4.2.2 网络安全

4.2.2.1 防火墙

防火墙技术可包括以下内容：

a) 基于状态检测的分组过滤，多级的立体访问控制机制；

b) 可支持多种连接方式、面向对象的管理机制和一次性口令认证机制；

c) 可支持 0SPF、IPX、NETBEUI、SNMP 等网络协议；

d) 具有带宽管理能力与远程管理能力，负载均衡；

e) 可支持动态 IP 地址，内嵌 VPN 功能支持；

f) 灵活的审计、日志功能。

4.2.2.2 检测入侵行为

网络入侵行为可包括以下内容：

a) 可在网络环境下进行实时、分布式，全面、协同、并行地检测所有的入侵行为；

b) 可按照需要进行多层次的扫描，及时发现、识别、有效阻断或弱化攻击行为；

c) 应建立相应的可强制执行的安全策略。具有帮助型数据库，协助管理网络的安全；

d) 检测和扫描行为不应影响网络的正常运行；

e) 可详细记录、生成入侵检测报告，及时报警。

4.2.2.3 数据传输安全

数据传输安全可包括以下内容：

a) 客户宜采用强制性身份认证，应保证数据传输的安全性；

b) 可采用 PKI 数字加密、签名等防伪技术；

c) 应对系统进行配置管理。

4.2.3 系统安全

4.2.3.1 操作系统

操作系统安全管理应包括登录安全、文件系统安全、注册表安全、远程访问服务安全、数据安全、应用系统安全等，制定强制性的措施。

4.2.3.2 数据库

数据库管理系统可包括以下内容：

a) 控制，利用 DAC 模型来决定客户访问数据库权限；

b) 验证，保证只有授权的合法客户才能注册和访问；

c) 授权，对不同的客户应授予不同的访问权限；

d) 审计，可监视各客户对数据库施加的动作，并能提供与安全相关事件的审计能力；

e) 标识，系统应提供在数据库级和记录级标识信息的能力。

4.2.4 应用安全

4.2.4.1 身份认证

对客户服务，如网上办事、网上咨询、网上投诉等，应当实行相应的身份认证服务。

4.2.4.2 病毒防范

病毒防范系统由防病毒代理和防病毒服务器端组成，应采用分布式运行和集中管理的方式。

4.2.4.3 响应与备份恢复

存储、备份、恢复可包括以下内容：

a) 可支持大容量存储，支持多种存储介质和备份模式；

b) 可支持异地备份与恢复，并具有跨平台的备份能力；

c) 可支持自动恢复机制。

5 系统建设要求

5.1 一般要求

一般技术要求可包括以下内容：

a) 系统主要采用 B/S 架构，兼容主流浏览器；

b) 构建统一的信息安全保障系统，提供标准的身份认证接口，通过权限管理、日志管理等多种技术手段保障系统安全运行；

c) 配置可视化应用接口，对系统运行进行管理、监控，并记录运行日志；

d) 系统各类应用为统一的单点登录。登录的信息在各系统间完全一致，同步变动；

e) 系统采用的软、硬设备应自主、可控。满足快速部署、简便灵活、便于扩充与延伸等要求。

5.2 易用性

系统的易用性可包括以下内容：

a) 可根据需求按必设和自选两类设置；

b) 考虑浏览器兼容性、字体兼容性和插件流行程度等；

c) 对于专业性较强的术语、复杂的操作应有在线帮助或操作指南；

d) 客户操作完每一步骤后，应提示当前所处状态；

e) 具有严重后果的功能执行应是可逆的。程序应给出严重后果的警告或提示，在执行命令前应再次确认。

5.3 安全性

系统的安全性可包括以下内容：

a) 统一规划、系统分析、完整设计，方案实用、系统可靠；

b) 系统网络结构设计、设备选型、安装调试等各环节要满足设计要求；

c) 应提供多层次安全控制手段，建立完善的安全管理体系，保证数据的完整性、保密性；

d) 应有可靠的防病毒、防篡改措施；

e) 采用工作日志管理方式，具有痕迹管理功能。对所有事项办理过程能够完整的还原，并具有抗抵赖性，角色权限划分等功能。

5.4 网站页面设计

网站页面设计可包括以下内容：

a) 页面整体设计风格一致，页面布局、用图与用色风格一致；

b) 接口元素命名一致，相同元素不应重复命名；同类元素的命名应保证一致性；

c) 相同功能宜使用相同元素；

d) 接口元素样式及摆放位置应在同一接口。不同接口之间要协调一致；

e) 不同栏目版面内容不宜有交叉重复内容，共性较多的内容应尽量划分到同一栏目版面上；

f) 层次结构不应超过 3 层；

g) 常用信息内容、功能服务宜放到较浅层次上；

h) 信息内容获取和功能服务过程不宜超过 3 步，当需要更多步骤时应有简单、明确提示。

5.5 域名设计

域名应容易理解和记忆，避免使用无意义的或难以理解的字符/数字组合很长的域名。

6 系统功能要求

6.1 管理平台

系统管理平台可包括以下内容：

a) 统一账号管理，为客户提供统一集中的账号管理，实现账号的创建、删除及同步；

b) 通过平台进行账号密码策略，密码强度、生存周期的设定等基本功能；

c) 统一认证管理，可根据客户的实际需要，提供不同强度的认证方式，实现客户认证的统一管理、访问的单点登录。

d) 不同强度的认证方式主要有：

1) 具有静态口令方式；

2) 高强度的双因子认证方式，如一次性口令、数字证书、动态口令等；

3) 新型的生物特征认证方式。

e) 统一权限管理，对客户的资源访问权限进行集中控制；

f) 统一审计管理，管理和分析客户操作日志的集中记录、监控客户行为，通过集中的审计数据进行数据挖掘。

6.2 分析平台

系统分析平台可包括以下内容：

a) 应满足系统整体流量分析的需要，内容应包括浏览量和浏览人的IP 地址、平均逗留时间、浏览页面数等；

b) 应提供图形化的年报、月报、周报、客户区域分析报告；

c) 对各项行政效率、工作绩效进行统计分析和绩效评估；

d) 为日常工作可提供决策或预测依据。

6.3 数据要求

6.3.1 分类

数据可按照文本、图形图像、音频、视频和动画等格式进行分类。

6.3.2 要求

数据应符合GB/T 15121.4、GB/T 17191.1、GB/T 17235.1、GB 18030、GB/T 2312的规定。

6.3.3 数据接口

数据接口可包括以下内容：

a) 数据接口系统的设计和制作应保证数据的一致性、系统的安全性、开放性和适用性；

b) 数据接口方式可包括基于 IP 的通信包交换、文件的数据交换、数据库表一级的交换；

c) 每一级数据交换，应定义接口数据的结构、格式、语义；

d) 信息服务标准化宜采用 XML 技术，可通过 SOAP 协议以 XML 方式进行数据同步。

7 系统运行管理要求

7.1 管理制度

7.1.1 安全管理制度

系统安全管理制度可包括以下内容：

a) 人员安全、设备操作安全、场地与设施安全、设备使用、技术文档管理等；

b) 操作系统和数据库安全、系统安全恢复、备份安全、异常情况、数据保密、应急响应、安全软件版本、信息审校、采录与发布等；

c) 系统安全状况的定期评估策略、审计管理、运行日志安全等。

7.1.2 岗位责任制度

岗位责任制度可包括以下内容：

a) 岗位设置、职责；

b) 人员配置、数量、条件标准、任职期限、风险机制、奖惩细则；

c) 人员聘用事项等。

7.1.3 网络管理制度

网络管理制度可包括以下内容：

a) 网络系统运行操作规程；

b) 运行过程监控管理；

c) 系统设备配置与更新管理；

d) 系统系统维护与报废管理；

e) 网络与信息系统安全应急响应；

f) 系统使用规定等。

7.1.4 信息管理制度

信息管理制度可包括以下内容：

a) 信息的采集、录用、审校与发布的管理；

b) 信息内容和服务项目及时发布与更新信息；

c) 不应出现知识性、文字性差错；

d) 所有信息不应选用、发布与国家方针、政策、宣传口径不一致，不应宣扬封建迷信、恐怖暴力、明显失实、泄密等稿件。

7.1.5 技术文档管理制度

技术文档管理制度应包括文件建立、保存、借阅及报废等。

7.2 安全审计

安全审计可包括以下内容：

a) 机构设置应包括机构设立、职能职责、人员配置、聘用与考核等；

b) 日志审计，可提供各个客户操作管理系统的痕迹跟踪功能。每一个登陆管理系统的客户，其对系统的任意修改，应被记录，包括增加、删除和变更。可有效控制和监管错误操作或者恶意攻击；

c) 审计人员应具有较强的法律意识、专业技术知识与技能；

d) 社会安全审计部门和人员应具有相应的安全审计从业资质。

7.3 网站日志

7.3.1 平台应当对客户访问、事项处理以及各级管理员操作维护工作进行详细记录，记录保存时间应不少于 6 个月，并提供统计、审计与分析功能。

7.3.2 日志记录应完整，包括系统监控、客户操作日志记录等。

7.4 技术保障服务

技术保障服务可包括以下内容：

a) 技术保障服务类别。可采用自行承担或服务外包两类，为服务系统的正常运行提供技术保障。采用服务外包方式的双方应签订服务保障协议或合同；

b) 技术保障服务承诺。应明确承诺内容，包括现场问题诊断、远程问题诊断、系统维修及维护与修复、产品升级服务和定期巡检服务等，并制定服务质量承诺书；

c) 技术保障方式。可提供 7×24 小时热线电话和远程维护。电子邮件和实时消息等进行远程维护及现场支持；

d) 运行报告制度。技术保障服务机构定期向管理部门报送运行《情况报告》，主要包括系统使用、业务量统计、故障处理、服务请求与响应等情况；

e) 故障分级响应机制。根据故障程度可划分为三个等级，系统根据不同故障等级，分别设定响应机制。

1) A 级故障为特大故障，对系统运行有严重影响，导致系统无法运行；

2) B 级故障为重大故障，限制了部分系统运行；

3) C 级故障为一般故障，对系统运行产生轻微影响，大部分系统仍可运行。

f) 服务质量考核机制。明确服务质量考核指针和评估方法，包括服务满意度、平均响应时间、投诉发生率等，根据评估结果对技术保障服务机构和服务人员进行奖惩和聘用；

g) 系统应用的岗位培训。技术保障服务机构要负责组织系统应用的技术培训、使用培训。

8 系统评测与验收要求

8.1 系统评测

系统评测可包括以下内容：

a) 系统构建完成后，可通过专业评测机构对平台功能和性能进行技术评测，并写出评测报告；

b) 服务评测。在服务正式上线后，应对服务系统运行情况和办件效率等内容进行定期评估。可采用方法分为网上测评、抽样检查和效率评估等。

8.2 系统验收

系统验收可包括以下内容：

a) 系统评测结束后，应组织各方面的技术专家、专家和有关的业务人员对服务系统进行验收；

b) 应用上线验收。在应用上线及延伸构建完成后进行验收。可采用技术测评和在线操作等方法，验收内容包括规范公开、服务事项、应用设计等。

三、主要试验和情况分析

结合国内外的行业测试标准和企业内部工厂管控的项目进行要求规定和试验验证。

四、标准中涉及专利的情况

无

五、预期达到的效益（经济、效益、生态等），对产业发展的作用的情况

企业服务管理系统设计规范运营，在国际市场上有机会与其他各国（相关）企业竞争。

六、与有关的现行法律、法规和强制性国家标准的关系

与现行法律、法规和强制性标准没有冲突。

七、重大意见分歧的处理依据和结果

标准制定过程中，未出现重大意见分歧。

八、标准性质的建议说明

本标准为团体标准，供社会各界自愿使用。

九、贯彻标准的要求和措施建议

无。

十、废止现行相关标准的建议

本标准为首次发布。

十一、其他应予说明的事项

无。