ICS
CCS 点击此处添加 CCS 号

团　　体　　标　　准

T/QGCML XXXX—XXXX

数字发售系统

Digital distribution system

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

全国城市工业品贸易中心联合会　　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专利的责任。

本文件由××××提出。

本文件由全国城市工业品贸易中心联合会归口。

本文件起草单位：

本文件主要起草人：

本文件为首次发布。

数字发售系统

1 范围

本文件规定了数字发售系统的术语和定义、基本要求、功能特性、性能要求、安全要求。
本文件适用于数字发售系统的设计和检验。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

数字发售系统 Digital distribution system
指用于在线发售数字产品、服务或虚拟商品的软件系统，包括但不限于电商平台、数字内容平台等。

4 基本要求

4.1 合法性与合规性

4.1.1 系统应确保所发售的数字产品具备合法的知识产权，不得侵犯他人的版权、专利权等。系统应建立完善的审核机制，对上架的数字产品进行合法性审核。

4.1.2 系统应遵守国家法律法规和行业规范，不得从事任何违法违规的经营活动。系统应建立完善的合规管理制度，确保业务操作的合规性。

4.2 真实性与准确性

4.2.1 系统应确保所发布的商品信息真实可靠，不得夸大其词或虚假宣传。商品信息应包括但不限于商品名称、价格、描述、图片等。

4.2.2 系统应确保交易信息的准确性，包括用户订单信息、支付信息、物流信息等。系统应建立完善的交易信息核对机制，确保信息的准确无误。

4.3 稳定性与可靠性

4.3.1 系统应具备高度的稳定性，能够长时间稳定运行，不出现宕机、崩溃等故障。系统应建立完善的监控和预警机制，及时发现并处理潜在的系统故障。

4.3.2 系统应确保数据的可靠性和完整性，防止数据丢失或损坏。系统应建立完善的数据备份和恢复机制，确保在数据丢失或损坏时能够及时恢复。

4.4 安全性与保密性

4.4.1 系统应具备良好的安全性能，能够抵御各种网络攻击和恶意行为。系统应建立完善的安全防护体系，包括防火墙、入侵检测、数据加密等措施。

4.4.2 系统应保护用户数据的隐私和安全，不得未经用户同意擅自收集、使用或泄露用户信息。系统应建立完善的用户数据保护机制，确保用户数据的安全性和保密性。

4.5 易用性与可访问性

4.5.1 系统应提供简洁明了、易于操作的界面设计，方便用户进行商品浏览、购买、支付等操作。

4.5.2 系统应支持多种终端设备的访问和使用，包括 PC 端、移动端等，满足不同用户的需求。

4.5.3 系统应考虑到特殊用户的需求，提供无障碍访问功能，确保所有人都能够方便地使用系统。

4.6 可扩展性与可维护性

4.6.1 系统应具备良好的可扩展性，能够根据业务需求进行功能扩展和升级。

4.6.2 系统应具备良好的可维护性，能够方便地进行系统维护、故障排查和修复工作。

5 功能特性

5.1 商品管理

5.1.1 商品上架与下架

5.1.1.1 系统应支持管理员或商家快速、便捷地上架新的数字产品，并设置相应的商品信息，如价格、描述、图片等。

5.1.1.2 当商品售罄、过期或需要调整时，系统应支持商品的下架操作，并可选择是否保留历史销售数据。

5.1.2 商品编辑与删除

5.1.2.1 系统应允许管理员或商家对已上架的商品进行编辑，包括修改商品信息、更换图片、调整价格等。

5.1.2.2 对于不再需要的商品，系统应支持删除操作，并可选择是否删除相关的销售数据和评价信息。

5.1.3 商品分类与搜索

5.1.3.1 系统应支持对商品进行分类管理，方便用户根据需求浏览和查找商品。

5.1.3.2 提供强大的搜索功能，支持关键词搜索、分类搜索等多种搜索方式，提高用户查找商品的效率。

5.2 用户管理

5.2.1 用户注册与登录

5.2.1.1 系统应提供用户注册功能，支持用户通过手机号、邮箱等方式进行注册，并设置密码保护。

5.2.1.2 提供多种登录方式，如账号密码登录、第三方账号登录，提高用户登录的便捷性。

5.2.2 用户信息管理

5.2.2.1 系统应支持用户查看和编辑自己的个人信息，如姓名、联系方式、收货地址等。

5.2.2.2 提供用户订单管理功能，允许用户查看自己的购买记录、订单状态、物流信息等。

5.2.3 用户权限管理

5.2.3.1 系统应根据用户角色设置不同的权限，如普通用户、商家、管理员等，确保系统的安全性和数据的保密性。

5.2.3.2 允许管理员对用户进行权限设置和修改，以适应不同的业务需求。

5.3 订单管理

5.3.1 订单生成与查看

5.3.1.1 系统应支持用户购买商品后自动生成订单，并允许用户查看自己的订单详情，包括订单状态、支付状态、物流信息等。

5.3.1.2 提供订单搜索功能，方便用户快速找到特定的订单。

5.3.2 订单支付与退款

5.3.2.1 系统应支持多种支付方式，如在线支付、货到付款等，满足用户不同的支付需求。

5.3.2.2 提供订单退款功能，允许用户在符合退款条件的情况下申请退款，并自动处理退款流程。

5.3.3 订单评价与反馈

5.3.3.1 系统应支持用户对购买的商品进行评价和反馈，帮助其他用户了解商品的真实情况。

5.3.3.2 提供评价管理和回复功能，允许商家对用户的评价进行回复和解释。

5.4 营销推广

5.4.1 系统应支持创建和管理优惠券活动，允许商家设置优惠券的发放条件、使用规则等。

5.4.2 提供多种促销活动方式，如满减、折扣、限时抢购等，帮助商家吸引用户和提高销售额。

5.4.3 系统应利用先进的推荐算法，根据用户的购买历史和浏览行为推荐相关的商品或服务。

5.4.4 提供个性化的推荐功能，提高用户的购物体验和满意度。

5.5 财务管理

5.5.1 系统应提供订单统计和报表功能，帮助商家了解销售情况、库存状况等关键信息。

5.5.2 提供多种统计方式和报表模板，方便商家进行数据分析和业务决策。

5.5.3 系统应支持订单结算和财务对账功能，确保商家和系统的财务数据准确无误。

5.5.4 提供结算周期、结算方式等灵活的配置选项，满足不同商家的需求。

6 性能要求

6.1 响应时间

6.1.1 系统应优化页面加载速度，确保用户在访问网站或应用时能够迅速加载所需页面。对于首页、商品详情页等重要页面，加载时间应控制在合理范围内，一般不超过 3 s。

6.1.2 系统应确保在用户进行购买、支付、下载等交易操作时能够快速响应。交易响应时间应控制在合理范围内，一般不超过 2 s，以提高用户体验和交易成功率。

6.2 并发处理能力

6.2.1 系统应能够支持高并发用户访问和交易请求，确保在大量用户同时访问时系统仍然能够稳定运行。系统应具备良好的并发处理能力，能够处理数万甚至数十万级别的并发请求。

6.2.2 系统应实现负载均衡策略，将用户请求分配到多个服务器或节点上进行处理，以提高系统的吞吐量和响应能力。负载均衡策略应能够根据服务器负载情况动态调整请求分配。

6.3 数据处理能力

6.3.1 系统应能够高效地存储和检索大量数据，包括商品信息、用户数据、订单数据等。数据库设计应合理，采用高效的索引和查询优化策略，确保数据检索的准确性和快速性。

6.3.2 在多用户并发操作的情况下，系统应能够确保数据的实时更新和同步，防止数据冲突和不一致。系统应采用合适的数据更新策略，如乐观锁、事务管理等，确保数据的一致性和完整性。

6.4 可扩展性

6.4.1 系统应采用可扩展的架构设计，能够方便地添加新的功能模块、服务器或节点，以满足业务增长和用户需求的变化。系统应具备良好的可扩展性，能够支持大规模并发用户访问和数据处理。

6.4.2 系统应能够识别并优化性能瓶颈，提高系统的整体性能。对于存在的性能瓶颈，系统应提供相

应的优化方案或建议，以便及时改进和升级系统。

6.5 容错与恢复能力

6.5.1 系统应具备良好的容错能力，能够在硬件故障、网络异常等情况下继续提供服务。系统应采用适当的容错策略，如冗余部署、故障转移等，确保系统的稳定性和可靠性。

6.5.2 在系统发生故障或异常时，系统应能够快速恢复并重新提供服务。系统应提供备份和恢复机制，确保在数据丢失或系统崩溃时能够迅速恢复数据和服务。

7 安全要求

7.1 网络安全

7.1.1 防火墙和安全隔离

7.1.1.1 系统应部署防火墙来限制对内部网络的访问，并阻止未经授权的访问尝试。

7.1.1.2 不同功能区域（如用户区、管理区、数据库区等）应进行逻辑或物理隔离，以减少潜在的安全风险。

7.1.2 入侵检测和防御

7.1.2.1 系统应实施入侵检测系统（IDS）和入侵防御系统（IPS），以检测和阻止潜在的恶意攻击和入侵行为。

7.1.2.2 定期对系统进行安全扫描和漏洞评估，及时发现并修复潜在的安全隐患。

7.1.3 安全通信

7.1.3.1 所有敏感信息的传输（如用户密码、交易数据等）应采用加密通信协议（如 HTTPS），确保数据的机密性和完整性。

7.1.3.2 使用强加密算法（如 AES、RSA 等）对数据进行加密处理，防止数据在传输和存储过程中被窃取或篡改。

7.2 数据安全

7.2.1 数据加密

7.2.1.1 对所有敏感数据进行加密存储，包括用户密码、交易数据、个人信息等。

7.2.1.2 使用安全的存储设备和技术（如 RAID、数据备份等），确保数据的可靠性和完整性。

7.2.2 数据访问控制

7.2.2.1 实施严格的数据访问控制策略，确保只有授权用户才能访问敏感数据。

7.2.2.2 使用基于角色的访问控制（RBAC）或基于属性的访问控制（ABAC）模型，根据用户的角色和属性授予相应的数据访问权限。

7.2.3 数据备份和恢复

7.2.3.1 定期对重要数据进行备份，并存储在安全可靠的地方。

7.2.3.2 制定数据恢复计划，确保在数据丢失或损坏时能够迅速恢复数据和服务。

7.3 用户安全

7.3.1 实施多因素身份验证（MFA）机制，提高用户身份验证的安全性。

7.3.2 根据用户的角色和权限授予相应的系统访问和操作权限。

7.3.3 对用户进行安全意识教育和培训，提高用户识别和防范网络攻击的能力。

7.3.4 提供安全提示和指南，帮助用户保护自己的账户和密码安全。

7.4 系统安全

7.4.1 定期对系统进行漏洞扫描和评估，及时发现并修复潜在的安全漏洞。

7.4.2 建立漏洞修复流程，确保漏洞得到及时修复和验证。

7.4.3 实施定期的安全审计，评估系统的安全性和合规性。

7.4.4 记录所有系统活动和用户操作日志，以便进行安全审计和故障排查。

7.4.5 建立安全事件响应机制，包括事件检测、报告、分析和处置等流程。

7.4.6 定期进行安全演练和应急响应测试，提高系统应对安全事件的能力。

7.5 合规性

7.5.1 系统应遵守所有适用的法律法规和行业标准，确保合法合规运营。

7.5.2 定期进行合规性检查和评估，确保系统符合最新的法律法规要求。

7.5.3 遵循数据隐私保护原则，确保用户数据的安全性和隐私性。

7.5.4 在收集、存储和使用用户数据时，应遵守相关的隐私保护政策和法规要求。