ICS 03.060
CCS A 11

Q/BSX

绍 兴 银 行 股 份 有 限 公 司 企 业 标 准

Q/BSX 0002-2025

绍兴银行生僻字服务企业标准

Rare Character Service Enterprise Standard

2026-1-12 发布　　2026-1-12 实施

绍兴银行股份有限公司发布

目　　次

前　　言

本文规定涉及的内容包括：绍兴银行生僻字服务相关标准。

依据《银行业客户服务中心基本要求》《信息安全技术个人信息安全规范》《金融行业信息安全等级保护评测服务安全指引》《金融服务生僻字处理指南》的要求，制定本规范。

——本次为第一次发布。

绍兴银行生僻字服务安全标准

1 范围

本部分规定了绍兴银行生僻字处理总体规范要求，以及提出了生僻字在信息系统里如何显示、输入、存储、传输和打印等方面的指导性方案。

2 规范性引用文件

JR/T 0253—2022 金融服务生僻字处理指南
GB 18030-2022 信息技术中文编码字符集

3 术语与定义

3.1 编码字符集 coded character set

是一种映射规则，用于建立该字符集中的字符与其编码之间的对应关系。

3.2 字库 font library

存储文字字形信息的数据集合，通常以ttf/otf/woff/ttc等格式的文件形式存在。

3.3 人口信息字库 font library of population information

公安部门针对人口信息（姓名、地名等）数据数字化而定制的字库。

3.4 用户自定义区 private use area

未在UCS正式标准中指定，而由用户之间的私人协议决定字符用途的一系列码点，使用三个编码区块：U+E000~U+F8FF、U+F0000~U+FFFFD、U+100000~U+10FFFD。。

3.5 一字多码 one character corresponds to multiple codes

部分PUA编码字符后来陆续被UCS收录而拥有正式编码，所以产生了一个字对应多个编码的情况。

3.6 生僻字 rarely userd Chinese characters

本文特指GBK字符集之外的汉字字符。

3.7 通用编码字符集 universal coded character set，简称 UCS）

由国际标准化组织与国际电工委员会（ISO/IEC）制定的通用编码字符集标准，编号为ISO/IEC 10646。

4 生僻字服务安全规范

4.1 安全技术规范

4.1.1 客户端程序

a) 客户端代码重大功能上线后进行严格的代码安全监测由第三方机构出示检测报告，行方进行漏洞修改再由第三方复测，检测通过后方可上线部署。
b) 客户端程序打包时进行代码混淆，具有抗逆向分析、抗反汇编等安全性防护措施，防范攻击者对客户端程序的调试、分析和篡改。

4.1.2 网络通信安全

4.1.2.1 通讯协议

a) 使用 SSL 协议，保护客户端与服务器之间所有连接，保证传输数据的机密性和完整性。
b) 使用负载均衡，保证客户单与服务器之间的连接分发，减轻服务器的运行压力。

4.1.2.2 网络架构安全

合理划分网络区域，并设立专门的生僻字区与办公网及其他网络进行隔离。维护与当前运行情况相符的网络拓扑图，并区分可信区域和不可信区域。采用waf防火墙技术拦截异常的网络访问，对非业务必须的网络数据进行过滤。互联网接入采用不同运营商线路，相互备份且互不影响。保证网络宽带和网络设备的业务处理能力具备冗余空间，满足业务高峰期和业务发展需要。

4.1.3 服务端安全

4.1.3.1 网路安全

a) 系统采用 HTTPS 协议通讯，接口采用 SM4 加密进行数据传输，并采用 token 令牌来做授权和验证，token 定时更新。
b) 不涉及展现客户信息以及客户信息、转账信息的存储、传输。

4.1.3.2 主机安全

a) 行内定期对互联网环境实施渗透测试与漏洞扫描工作。业务部门、软件开发部需定期对系统漏洞实施修复。
b) 系统使用 https 协议进行通讯，接口采用加密和令牌进行授权和验证，保证传输过程中的链路安全。
c) 防 SQL 注入，采用预编译语句集，内置了处理 SQL 注入的能力，且采用过滤特殊符号、使用正则表达式过滤传入的参数、绑定变量，保证数据库安全。
d) 接口白名单模式。

4.1.3.3 应用安全

身份认证安全

a) 生僻字服务平台云字库不涉及用户登录，通过 token 进行使用认证，每天动态更新 token。
b) 生僻字服务平台后管服务涉及内管用户，有独立的登录功能，用户量较小。

移动客户端安全

a) SDK 使用安全设计：
b) （1）封装 WebView 的 js 与 java 互相调用的接口，防止 js 恶意注入。
c) （2）HTTPS 接口采用 token 验证，防止链接盗刷，参数使用加解密。

4.1.4 数据安全及备份恢复

a) 采用双秘钥机制（使用授权的 mid 和 key 请求 token 令牌，接口使用保护秘钥加密返回 token 令牌和 token 验证码），token 定时更新。
b) 生僻字数据库定期进行备份，可排除日志相关的表，并将备份上传专用的存储服务器，存储服务器进行异地备份。

4.2 安全管理规范

4.2.1 安全管理机构

a) 设立有专门的产品设计，系统研发、测试、集成、运行维护、管理等部门和团队。
b) 实现了三分离原则，实现前后台分离、开发与操作分离、技术与业务分离。
c) 加强风险管理文化建设，提高相关业务人员风险意识和思想道德准则，确保风险管理工作落到实处。

4.2.2 安全策略

a) 制定业务运行应急预案和安全策略，安全策略包括：对安全属性进行的重点规划、建设和管理，确保生僻字系统的机密性、完整性和可用性。
b) 建立信息安全风险的持续监测机制，制定风险预警、报告、响应和处理机制，实现生僻字安全风险监测的自动化，保证及时获取生僻字信息安全风险变化。
c) 制定生僻字信息交换的统一标准，明确生僻字在数据传输、接口交换、跨系统共享过程中的编码格式、数据结构规范、校验规则及异常处置机制，确保跨平台、跨业务的生僻字信息交换具备一致性、准确性和操作性，规避信息丢失或传输错误问题。

4.2.3 管理制度

建立系统设计、编码、测试、集成、运行维护等过程，并涵盖安全规范、操作记录手册等方面的信息安全管理制度体系。

4.2.4 系统建设管理

a) 开发环境与实际运行环境物理分开，禁止开发、测试在生产环境中进行，将开发人员与测试人员分离，开发人员不能兼任系统管理员或业务操作员，以确保测试数据和测试结果受到控制。
b) 制定了软件开发代码安全规范，明确开发过程的控制和人员行为准则，要求开发人员参照规范编写代码。
c) 应用开发及变更过程中，需完成项目计划、会议纪要、运维手册、测试案例等相关手册的编写工作，保证相关资料的完整性和准确性。

4.2.5 系统运维管理

a) 建立了机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定。
b) 指派专人担任机房管理员，对机房的出入进行管理，定时巡查机房运行状况，对机房供配电、空调、温湿度等设施进行维护管理。
c) 机房所在区域安装 24 小时视频监控录像装置。
d) 落实设备登记工作，制定了设备管理规范，落实了设备使用者的安全保护责任。

4.3 客户体验

4.3.1 服务体验

绍兴银行为生僻字提供7*24小时服务，包括电话服务和现场服务。自助服务支持自助挂失，人工服务支持人工挂失、业务咨询、业务指导和投诉处理。

4.3.1.1 服务响应

a) 系统设有专门的技术人员解决来自客户技术方面的问题，并实行首问责任制，提高事件处理效率。
b) 邮件支持服务：7x24 接受服务申请，服务团队将在 15 分钟内给予回复；
c) 电话技术支持：7x24 的技术支持服务，当联系电话变更时提前 3 个工作日进行通知；
d) 网络技术支持：7x24 接受各种服务申请，技术支持团队和甲方服务团队将在 15 分钟内给予回复；
e) 现场服务时间：在项目实施过程中，项目成员将根据行内工作要求，双方协商一致，提供一定时间的驻场服务。

4.3.1.2 服务性能

a) 在生僻字系统开发部署中，需保证系统在高并发场景下，以及大量用户请求的场景下稳定运行。生僻字应用处理平台需支持 7*24 小时持续、稳定运行，业务异常中断时不能影响其它业务功能的正常开展，升级过程中对用户无影响。