



ICS 03.060
A11

Q/HH

新疆汇和银行股份有限公司标准

Q/HHBANK 001—2021

新疆汇和银行网上银行服务标准

Xinjiang Huihui Bank Online Banking Service Enterprise Standards

2021 - 07 - 19 发布

2021 - 07 - 20 实施

新疆汇和银行股份有限公司 发布



企业标准信息公共服务平台
公开 2021年07月23日 19点09分

企业标准信息公共服务平台
公开 2021年07月23日 19点09分



目 次

前 言.....	6
1 范围.....	3
2 规范性引用文件.....	3
3 术语与定义.....	3
4 网上银行业务功能概述.....	4
5 网上银行安全情况概述.....	6
6 网上银行客户体验概述.....	9
参考文献.....	11

企业标准信息公共服务平台
公开
2021年07月23日 19点09分



BANK 001—2021

前 言

本标准根据 GB/T 1.1—2009《标准化工作导则》给出的规则起草。

本标准根据 JR 0068—2012《网上银行系统信息安全通用规范》、JR/T 0071—2012《金融行业信息系统信息安全等级保护实施指引》、GB 32125—2015《银行业客户服务中心基本要求》、GB/T 35273—2017《信息安全技术个人信息安全规范》以及《电子银行业务管理办法》、《支付结算办法》和《汇和银行电子银行章程》等相关规定制定。

本标准由新疆汇和银行股份有限公司提出并归口。

本标准起草单位：新疆汇和银行股份有限公司。

本标准主要起草人：樊明华、郝盼盼。

企业标准信息公共服务平台
公开
2021年07月23日 19点09分



新疆汇和银行网上银行服务企业标准

1 范围

本标准规定了网上银行运营环境、系统架构、服务顾量、业务类型、风险管理、投诉处理和业务操相关内容,明确了网上银行运维标准、安全情况、客户体验及实施保障等内容与要求。

本标准适用于汇和银行所有网上银行业务。

2 规范性引用文件

下列文件对于本企业服务标准的应用是必不可少的,凡是注日期的引用文件,仅所注日期的版本适用于本文件。凡是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 35273-2017 信息安全技术个人信息安全规范

GB/T 32315-2015 银行业客户服务中心基本要求

JR/T 0170-2020 个人金融信息保护技术规范

JR/T 0068-2012 网上银行系统信息安全通用规范

JR/T 0071-2012 金融行业信息系统信息安全等级保护实施指引。

3 术语与定义

3.1

网上银行 Online banking

网上银行是传统银行业务系统的扩充和延伸。商业银行等金融机构通过互联网、移动通信网络、其他开放性公众网络或专用网络基础设施向其客户提供的网上金融服务。

3.2

网上银行业务 Online banking buslnese

网上银行业务是指借助电或其他智能设备,通过互联网技术或其他公用信息网,为客户提供的多种金融服务。网上银行业务又分为个人网上银行和企业网上银行。

3.3

网上银行客户 Online banking clients

与我行签订服务协议并开通网上银行业务的客户,包括个人客户和单位客户。

3.4



BANK 001—2021

网上银行数字证书 Digital Certificate in Online Banking

网上银行数字证书是指由中国金融认证中心发放,包含了证书持有人身份信息以及公开密钥等相关信息,用于证实客户身份、保证网上信息安全,且能确认持有人唯一身份的电子文件。

3.5

转账汇款 Transfer of remittances

客户通过网上银行向本行或他行账户办理的资金汇划业务。

3.6

账户Account

客户在我行开立的人民币结算账户。

3.7

网上支付 Online Payment

客户通过网上银行办理的话费充值、水电燃气缴费等在线支付业务

3.8

贷款Loan

客户通过网上银行办理的贷款申请、贷款查询、放款、还款等业务。

3.9

客户服务Customer service

我行为网上银行客户提供的操作日志查询、权限管理、登录密码修改等业务。

3.10

业务复核 Operational review

企业网银复核员对录入员提交的业务办理申请进行二次审核。

4 网上银行业务功能概述

汇和银行网上银行的功能随着业务产品的开发和网上银行系统的不断升级而逐步扩展本行网上银行分为大众版和专业版两种。

4.1

大众版网上银行功能概述

大众版网上银行提供账户信息查询、账户管理、存款计算器、等功能。



账户信息查询包括账户状态、账户余额和历史交易明细查询等。
账户管理包括关联账户管理、账户挂失。

4.2

专业版网上银行功能概述

4.2.1 个人网银服务功能

- a) 转账汇款
单笔转账、批量转账、定时转账、实时转账、转账管理、协议管理、交易撤销、手机号码绑定及转账
- b) 查询服务
总资产查询、账户信息查询、交易明细查询、转账状态查询、贷款账户查询、他行账户查询、电子工资账单查询、电子回单查询
- c) 投资理财
定活互转、通知存款、特色业务、理财产品购买、理财产品撤销、理财持有赎回、理财风险评估、理财签约/解约
- d) 特色业务
无卡取款
- e) 网银管理
账户管理、登录设置、安全管理、个性设置、个人信息管理、移动银行管理

4.2.2 企业网银服务功能

- f) 查询服务
余额查询、明细查询、资产负债查询、转账状态查询、未授权交易查询、银企对账查询
- a) 交易录入
单笔转账、批量转账、代发工资、定时转账签约、银企对账
- b) 交易审核
交易授权
- c) 票据业务
电子票据签约、票据业务签收、出票、背书转让、提示付款等。
- d) 投资理财
通知存款购买及支取、理财签约/解约、理财产品查询、理财产品购买、理财产品撤销、持有产品赎回、理财风险评估

4.2.3 账务查询功能

对公及个人存款账户行内转账、跨行转账、代发工资、基础理财、实时交易查询、账户状态、历史交易明细查询、贷款账户余额、本人授权他人支付、他人授权本人支付、手机号码转账等。

行内转账只限收款方为汇和银行账户。

跨行转账收款方为他行账户,支持 100 万元以下(含 100 万元)实时到账,100 万元以上普通转账,同



BANK 001—2021

时可以选择次日到账

4.2.4 银行交易功能

银行交易功能包括行内转账、跨行转账、批量转账、代发工资、定时转账、基础理财、投资理财、手机号码支付等功能。其中“定时转账”是指在网上银行上约定转账时间进行转账；“基础理财”包括个人活期转活期、个人定活互转；个人活期转活期是指挂在同一网上银行用户下的活期存折/卡之间的资金互转；个人定活互转是指网上银行用户同一银行卡内的活、定期资金互转；“投资理财”包括理财产品购买、理财产品撤销、持有产品赎回、理财风险评估，即可以通过网上银行购买我行理财产品，同时可赎回、撤销；手机号码支付是指依托网上支付跨行清算系统（“超级网银”）的新增功能，用户通过手机号码与常用银行账号进行绑定注册，后续的转账过程中即可以手机号码要素代替账号要素，实现在不输入账号的情况下，通过输入手机号码完成支付转账。

4.2.5 账户状态管理功能

账户口头挂失、修改密码、账户关联、设定交易授权等

4.2.6 个性化定制功能

电子回单打印及验证、网上留言、预约服务等。

4.3

其他服务功能

4.3.1

网上银行业务账务处理、资金清算纳入本行核心业务系统。网上银行资金清算时间：行内转账实时清算，跨行转账按人民银行大小额支付清算系统，网上银行互联系统的清算时间。

4.3.2

网上银行根据注册客户的电子指令为其办理转账付款等业务根据电子指令生成电子回单，网上银行用户可自行打印。

4.3.3

网上银行落地业务是指网上银行客户在网上发起转账，转出账户处理需由银行网上银行后台管理人员参与的业务，网银后台管理人员必须及时处理在营业时间内收到的落地业务，不得无故拖延落地业务的审核，实时业务实时通知。

5 网上银行安全情况概述



5.1 安全认证技术

5.1.1 数字证书

客户端采用 X509 证书,使用户可对交易做数字签名,从而实现不可否认性(Non-repudiation),对大额金融交易,特别是企业用户,是不可或缺的。需要澄清的是,这个“不可否认性”,是密码学里的一个数学特征,并不意味着法律效力或约束力。具备了数字签名,无非是说明持有证书私钥者做了这笔交易,至于私钥是否已被窃取,系统在挂失前很难测知。

5.1.2 登录密码

采用双因子认证,而其中一个因子仍是登录密码,恐怕一时难以改变。即便如此,对登录密码的管理、设置、存贮仍有一系列安全要求。例如对密码的强度和复杂性做检查,要求定期更换,采用软键盘防止盗号木马等措施。

5.1.3 动态口令

个人客户在登陆手机银行进行交易时,通过输入“密码”+“手机动态口令”多因素志认证的方式增强安全性,手机动态口令每隔一分钟就会产生一个新的密码,不可预测,并只能使用一次:所以不怕“重放攻击”,不易破解,具有很高的安全性和使用方便性。

5.1.4 短信认证

个人客户在登陆手机银行进行交易时,通过输入“密码”+“短信验证码”方式,短信发送到客户预留手机号码中,短信验证码是根据专门的算法,每隔60S生成一个与时间相关、不可预测的随机数字组合,每天可产生43200个密码。

5.1.5 云证通

云证通是汇和银行与中国金融认证中心(CFCA)进行合作,联合推出的全新数字证书技术,云证通以 SDK 方式集成到已有的 APP 中,用户无需下载额外的 APP 应用;采用自主研发的分散式密钥签名算法,保障用户交易安全;金融级安全基础设施,云服务运营环境安全可靠。客户只需在手机银行 APP 安装该证书,无需借助动态令牌,即可随时随地实现大额转账。

5.2 网上银行系统安全管理

5.2.1 加强网络安全防护能力

清算中心的整个网络有较高的先进性和安全性,网络拓扑结构合理,设备性能满足业务高峰期需要。一是石泉机房、数讯机房、金电机房共有 7 条互联网接,能够提供各行客户冗余稳定的互联网访问;二是清算中心对于成员行的连接也提供了石泉机房和金电机房 2 个运营商 4 个专线的接入,以保证电子银行客户不间断的访问;三是整个网络的硬件设备 90%以上提供了双机双电的冗余备份,对网络的正常可靠的运行提供了保证;四是在网络安全方面在网络边界部署 IPS 设备、DDoS 设备、多层异构防火墙并配



BANK 001—2021

置了严格的访问控制策略来保证访问网络内主机的安全。

5.2.2 提升主机系统高可用性

清算中心的电子银行系统的数据库和中间件主机使用了 M-P 系列高端服务 (IBMP750 或 P740 小型机), 数据库服务器主机安装 HACMP 集群软件实现了双机热备高可用性, 应用中间件服务器通过 HACMP 或硬件负载均衡方式保证了高可用及冗余。

服务器在身份鉴别、访问控制、安全审计方面较为完善: 服务器中不存在未删除的多余、过期账户用户登录堡垒机时使用实名账户, 不存在共享账户。具备堡垒主机, 运维人员进行远程运维操作需使用实名账户先登录堡垒机, 堡垒机通过用户名、口令结合动态令牌的方式进行身份鉴别。服务器通过角色访问控制权限保护服务器的审计进程。服务器开启 `syslogd` 审计守护进程, 且 `wtmp`、`faillog` 等均为系统默认日志, 无法进行中断。

5.2.3 完善数据安全及备份机制

电子银行系统采用 HTTPS 协议, 具备保证传输过程中数据完整性、保密性的功能。敏感的用户信息, 如 PIN 码在数据库中加密存储。数据库数据、系统日志信息每日全量备份, 通过 NBU 实施备份, 并每日导入磁带中保存。建立了重要数据的定期数据备份机制。核心层, 汇聚层的设备和重要的接入层设备均采用双机热备部署, 通信线路采用电信和联通。

5.2.4 深化与推进流程管理

事件管理重点对流程和管理细则进一步深化与推进, 切实与相关考核机制进行关联, 明确了相关的职责、上报及通报机制、及事发、事中、事后的信息报告及时更新机制, 加强与业务部门沟通、交流完善事件处理流程中科技部门与业务部门的职责分工。

问题管理的重点工作将整体工作前移, 主动发现问题, 巩固问题输出的成果, 加强与其他服务流程间的联动, 将问题诊断解决的方案形成优化建议与知识库条目, 输出到其他服务流程中, 变更管理将着力优化变更流程, 缩短多重审批流程, 减少变更类型, 按照中心现有的组织架构进行优化调整; 从多级审批缩短至两级审批, 以提高变更流转效率。

5.2.5 完善信息安全管理, 加大信息安全检测深度

依据监管及信息安全管理的要求, 结合清算中心实际, 融合清算中心现行的信息安全制度和流程, 形成可持续发展的信息安全管理机制。

积极开展第三方安全测试工作, 以人民银行和银保监会和发布的标准为依据, 实施信息安全测评工作, 揭示信息安全存在的问题和不足, 提出信息安全工作改进建议。

通过漏洞扫描工具以本地扫描的方式对系统和网络进行安全漏洞扫描, 从内网和外网角度来查找网络结构、网络设备、服务器主机、数据和用户帐号/口令等安全对象目标存在的威胁。检测出目标系统中存在的安全漏洞, 如缓冲区溢出漏洞、系统弱口令漏洞、漏洞及操作等。对漏洞信息进行分析并制定整改方案, 持续跟踪。

通过渗透测试检测清算中心电子银行系统直接暴露在互联网上的安全隐患, 并提供实际可行的安全修复建议。通过本地渗透测试检测清算中心电子银行系统面向接入行的安全隐患, 并提供实际可行的安全修复建议。



5.3 网上银行个人信息保护

网银客户端安全措施

- a) 新客户初次使用网银系统,需要重新设置网银系统登录密码,在设置密码时提示客户设置复杂度较高的密码;
- b) 交易密码加密传输,防止泄露明文密码;
- c) 网上银行安全控件能够有效的防止木马、病毒等非法程序窃取用户的账户密码和交易信息,保证用户的账户安全;
- d) 客户在登录网银时登录密码输错三次,会提示稍后再试,不允许多次试密;
- e) 预警机制:异地登录及频繁登录则会触发网上银行预警机制,进行提示。必要时进行暂时锁定需联系开户行;
- f) 客户可设置防伪密码,可以预设防伪标志;
- g) 客户退出网银后不残留信息,安全退出后需要重新登录才能进行操作;
- h) 网银安全控件和移动银行 APP 具有反编译、篡改改、防劫持、防扫描等安全加固功能。

5.4 网上银行服务连续性

网上银行系统服务时间满足 7×24 小时不间断运行,配备 7×24 小时运维应急人目前清算中心共有三个数据中心,以上海石泉数据中心为主生产,上海数讯数据中心为同城应用级灾备中心,北京金电数据中心为数据级异地灾备中心,建成了清算中心的“两地三中心”灾备防御体系。RPO≈0,RT0≤30 分钟。系统及应用可用性监控覆盖率为 100%。

5.5 网上银行身份认证管理

5.5.1 手机网银

手机网银登录需要输入登录密码,用户进行交易时必须输入交易密码并且可以选择短信认证、云证通或者动态口令(三者必选其一)进行验证。验证方式如下:

登录密码+交易密码+动态口令

5.5.2 PC 网银

PC 端一代个人网银登录需要输入登录密码,客户进行交易时需要输入交易密码,并且通过数字证书进行安全认证。认证方式如登录密码+交易密码+数字证书

- a) 登录:登录密码输入 3 次则暂时锁定,超过 6 次需柜面解锁;
- b) 退出:5 分钟不使用网银则自动退出至登录界面;
- c) 预警机制:异地登录及频繁登录则会触发网上银行预警机制,进行提示。必要时进行暂时锁定需联系开户行;
- d) 客户可设置防伪密码,可以预设防伪标志;

5.6 风险控制能力



BANK 001—2021

对于网上银行业务涉及的敏感信息在通信过程做了加密操作,系统存储中需要保密的数据采取保密。

- a) 支付敏感信息在使用完毕后,立即进行清除;
- b) 确保无法通过技术手段恢复已清除的支付敏感信息;
- c) 网上银行利用大数据分析、用户行为建模等技术,对接用户行为分析系统,对客户的交易做了埋点监控,以便日后建立交易风险监控模型和机制;
- e) 网上银行系统具有详细的交易流水查询功能,包括但不限于日期、时间、交易卡号、交易金额和资金余额等信息;
- f) 网上银行系统具有账户信息变动提醒功能,可使用手机短信方式实时告知客户其账户的资金变化重要信息。

6 网上银行客户体验概述

客户体验是一种纯主观的在用户使用产品过程中建立起来的感受。良好的用户体验有助于我行不断完善产品或服务。正是这所有用户接触的感受差异,让我们对客户体验变得尤为重视。

6.1.1 个人网上银行业务规定

- a) 个人网上银行注册、变更、注销可由本人自助注册或到营业网点柜面办理,不可代办;
- b) 未开通 USB Key 的客户可使用账户查询、贷款查询等部分个人网上银行功能。已开通 USB Key 的客户可使用所有个人网上银行功能;
- c) 同一身份证件号码只能注册一次网上银行,其他同名账户可作为下挂账户使用;
- d) 客户在营业网点柜面办理个人网上银行业务必须由本人持有效身份证件办理且年满 16 周岁(含)未满 16 周岁不得为营业网点柜面办理个人网上银行业务;
- e) 各业务所属管理部门在个人网上银行所提供的产品和服务中的所有内容应符合国家相关法律法规的规定,包括但不限于文字内容、字体、图片、视频、动画等,须保证在个人网上银行使用时不存在权利上的瑕疵,不会发生侵犯第三方知识产权的情况,且不会发生其他违法违规情形;

6.12 企业网上银行业务规定

- a) 客户申请开通企业网上银行功能时,必须已在本行开立基本存款账户或一般存款账户。
- b) 申请代发工资功能的客户,必须已开立基本存款账户,并已签订网上银行代发工资业务协议;
- c) 企业在我行一个网点开有结算账户的,只能在开户行注册网上银行。企业在我行多个网点开立有结算账户的,需要前往客户号所在网点进行网上银行注册。信息变更、操作员管理及销户业务需至客户号的开户行办理。



参 考 文 献

- JR/T 0068-2012 《网上银行系统信息安全通用规范》
JR/T0071-2012 《金融行业信息系统信息安全等级保护实施指引》
GBT32125-2015 《银行业客户服务中心基本要求》
GB/T35273-2017 《信息安全技术个人信息安全规范》
《电子银行业务管理办法》
《支付结算办法办法》
《新疆汇和银行电子银行章程》
-

企业标准信息公共服务平台
公开
2021年07月23日 19点09分