CCS 03.060
A11

Q/NXB

宁夏银行网上银行服务企业标准

Q/6401000NXYH-002-2021

宁夏银行网上银行服务标准

Internet Banking service standards of NingXia-Bank

企业标准信息公共服务平台
公开 2021年07月30日 15点52分

2021－07－30 发布　　2021－07－31 实施

宁夏银行股份有限公司　　发布

目　　次

前言 II
引言 IV
1 范围 1
2 规范性引用文件 1
3 规范性法律法规 1
4 术语与定义 1
4.1 网上银行 2
4.2 静态密码 2
4.3 认证要素 2
4.4 认证方式 2
4.5 电子指令 2
4.6 身份证件 2
4.7 数字证书 2
4.8 网上银行服务对象 2
4.9 网上银行版本..... 2
4.10 网上银行交易验证.....3
4.11 网上银行交易记录 3
4.2 落地业务..... 3
5 服务安全 3
5.1 基本安全要求 3

5.2 业务服务连续性 3
5.3 交易认证及安全防范要求 3
5.4 风险防控能力 4
5.5 安全技术规范要求.....4
6 服务功能 7
7 服务性能 8
8 服务体验 8
8.1 客服人员行为规范 8
8.2 客服人员工作操守 8
8.3 客户服务规范 8
8.4 柜面人员客户服务 9
8.5 业务主管部门职责 9
9 服务保障 9
9.1 组织保障 9
9.2 制度保障 10
9.3 培训保障 10
9.4 业务检查 10
9.5 客户隐私保.....11

前　言

本标准依据 GT/T 1.1—2009 规则起草，依据 GB-T1.1-2020 规则修订。

本标准由宁夏银行股份有限公司提出。

本标准起草单位：宁夏银行股份有限公司。

本标准主要起草人：张立达

企业标准信息公共服务平台
公开 2021年07月30日 15点52分

引　　言

本标准内容涉及服务安全、服务功能、服务性能、服务体验、服务保障五个方面，旨在明确网上银行服务企业标准，促进网上银行健康发展。

企业标准信息公共服务平台
公开　2021年07月30日 15点52分

宁夏银行网上银行服务企业标准

1 范围

本标准规定了宁夏银行股份有限公司（以下简称“宁夏银行”）向客户提供的网上银行服务时，在服务安全、服务功能、服务体验、服务保障等方面应满足的规范要求。

本标准适用于本版本发布之日宁夏银行股份有限公司提供的网上银行服务。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。

GB 1.1-2009 标准化工作导则

GB/T 35273-2017 信息安全技术 个人信息安全规范

GB/T 19000-2016 质量管理体系 基础与术语

GB/T 32319-2015 银行业产品说明书描述规范

JR/T 0068-2019 网上银行系统信息安全通用规范

JR/T 0071-2020 金融行业网络安全等级保护实施指引

JR/T 0072-2020 金融行业网络安全等级保护测评指南

JR/T 0105-2014 银行数据标准定义规范

JR/T0118-2015 金融电子认证规范

3 规范性法律法规

下列文件对于本文件的应用是必不可少的。

中华人民共和国商业银行法

中华人民共和国电子签名法

中国人民银行人民币银行结算账户管理办法

中国人民银行支付结算办法

中国人民银行网上银行系统信息安全通用规范

中国银行业监督管理委员会电子银行业务管理办法

商业银行业务连续性监管指引

4 术语与定义

JR/T 0068-2019、GB/T 32315-2015、GB/T 35273-2017、GB/T 19000-2016界定的以及下列术语和定义适用于本标准。

4.1 网上银行

宁夏银行通过互联网、移动通信网络、其他开放性公众网络或专用网络基础设施，能够在任何时间、任何地点、以任何方式向其客户提供自助式金融服务，具有转账汇款、网上支付、信息查询、投资理财、缴费支付等功能。

4.2 静态密码

在网上银行服务中由客户自行设定的一组用于识别客户身份的字符、数字信息。通常有登录密码、交易密码、数字证书（USBKey）PIN码等。

4.3 认证要素

在网上银行交易中，宁夏银行用于识别客户身份的信息要素。如客户号、用户名、银行卡号、对公账号、证件号码、静态密码、数字证书、签约注册的手机号码或其他与银行约定的身份识别编码等作为识别网上银行客户有效身份识别标识，凡使用正确的客户身份识别标识和身份认证方式进行的交易均视为客户本人所为，所产生的电子信息记录为该项交易的合法有效凭据。

4.4 认证方式

指数字证书认证、静态密码认证、短信验证码认证等。宁夏银行根据网上银行业务类型的不同，提供一种或多种认证方式供客户选择。

4.5 电子指令

指客户通过网上银行渠道发出的查询、转账、缴费、理财等交易的信息指令。

4.6 身份证件

居民身份证或者临时居民身份证、军人身份证、武装警察身份证、港澳居民往来内地通行证、台湾居民来往大陆通行证或者其他有效旅行证件、护照等。

4.7 数字证书

指宁夏银行向国内权威 CA 机构中国金融认证中心（CFCA）申请的符合《电子签名法》的签名认证数字证书，用于在交易中识别客户身份以及保障交易、资金、信息安全。存放数字证书的介质是 USB-Key。

4.8 网上银行服务对象

网上银行服务对象是在本行开立结算账户的个人和企事业单位客户（以下简称企业），与本行签订网上银行服务协议、办理了网上银行注册手续。本行根据不同的客户类型和申请业务，遵循审慎原则为客户提供相应的网上银行产品和服务。

4.9 网上银行版本

个人网上银行为个人客户提供证书版网上银行，企业网上银行为客户提供证书版和查询版网上银行，证书版网上银行提供了查询、转账、理财、缴费等功能，查询版仅提供账户余额、交易明细查询等查询类功能。

4.10 网上银行交易验证

本行网上银行向客户颁发预植中国金融认证中心（CFCA）数字证书的USBKey保障交易的安全。客户通过使用数字证书（USBKey）认证方式登陆个人网银、企业网银证书版网银，交易时必须采用本行向其颁发的CFCA数字证书完成数字签名认证。

4.11 网上银行交易记录

客户在网上银行系统进行交易所产生的电子信息记录为交易记账的有效凭据，由此所产生的记账记录凭据作为电子信息记录处理，并在网上银行系统进行长期保存。

4.12 落地业务

指客户登录网上银行并发起交易后，超过约定限额，需由注册行工作人员进行落地审批处理的业务。

5 服务安全

5.1 基本安全要求

本行网上银行的安全技术、安全管理、业务动作安全、个人信息保护等均符合《GB/T 35273-2017 信息安全技术 个人信息安全规范》、《JR/T 0068-2012 网上银行系统信息安全通用规范》和《JR/T 0071-2012 金融行业信息系统信息安全等级保护实施指引》的规定。

5.2 业务服务连续性

本行网上银行系统服务时间满足7×24小时不间断服务。

本行网上银行系统配备7×24小时运维应急人员值班。

本行网上银行系统截止报告日末发生数据丢失及重大安全风险情况。

本行网上银行系统突发应急事件恢复时间按突发应急事件级别要求恢复时间分别为I级4小时以内，II级3小时以内，III级2小时以内。

本行网上银行系统可用性监控覆盖率达100%，监控覆盖网上银行实时业务、机房动环、硬件设备、操作系统、数据库、中间件、主机进程、网络连通性、文件系统存储空间、网络安全日志、业务异常分析、网络安全时间等实时监测。

本行网上银行已制定网上银行业务运营中断突发事件专项应急预案，及时有效处置网上银行业务原因中断突发事件。

5.3 交易认证及安全防范要求

5.3.1 交易认证

本行网上银行系统采用数字证书认证技术增强客户交易安全，交易流程采用单笔及累计交易落地限额、单笔及每日最大限额保障客户资金安全。本行根据客户类型、认证方式的安全强度，匹配相应的交易限额。

基于数字证书（USBKey），个人客户单笔及累计落地100万元，日累计最高限额为500万元。

企业客户单笔及累计落地限额为500万元，日累计最高限额为5000万元。个人客户可通过网上银行自行设置限额，但不得高于上述最高限额标准。企业客户前往网银注册行修改默认限额。

当客户使用数字证书（USBKey）进行交易时，应将交易的关键信息（账号、金额、交易时间、对方信息等）完整显示在USBKey显示屏上，客户根据显示信息完成交易的确认操作。

5.3.2 辅助安全认证

本行个人网上银行提供手机、计算机绑定辅助安全认证手段，绑定手机后可自行设置短信限额，超过限额的交易需通过绑定手机发送的验证码验证码认证后方可继续执行；计算机绑定后客户仅能在指定的计算机登录网上银行。

5.3.3 交易流程控制

本行采用完整的交易流程控制，当客户交易超过约定落地限额时，由网银注册行非业务处理人员采用双线认证核实方式与客户预留法人或大额资金联系人核实交易情况，包括交易种类、收款人信息、金额等。

5.3.4 交易安全防范要求

客户端与服务端全程采用双向SSL加密安全链路通讯，通讯过程中(数字证书）USBKey必须一直保持插入状态，插入数字证书时应自动弹出网银登录页面，防范钓鱼网站；拔掉数字证书后应断开交易链接，避免客户信息被泄露。服务器端及报文传输全流程应具备数据防篡改机制，确保客户所办理的业务交易信息与网上银行系统执行的交易指令保持一致，同时，网上银行交易页面具备防重复提交机制。

客户网银登录界面，当客户输入错误身份认证信息，在错误提示中没有明确错误原因，可有效增大暴力破解客户信息的难度。同时，对于连续输错静态密码（包括网上银行登录密码等）的情况，采取相应保护措施，包括但不限于锁定登录密码、短息通知绑定手机号码等安全机制。

提供网银助手等快捷辅助工具，提供客户检测、修复网银登录环境，故障检测等功能。

客户办理网上银行相关业务时，采用数字证书PIN码+数字证书确认，USBKey采用级别更高的二代USBKey,在屏幕上回显客户信息，由客户自主确认，方可提交，防范黑客远程控制。

5.4 风险防控能力

本行网上银行系统已接入反洗钱系统、黑灰名单管理和网络查控统一管理平台，在客户办理网上银行相关业务时进行客户洗钱风险级别检测、预警，交易环节嵌入黑灰名单控制黑灰名单管理检测，对黑灰名单客户的收付款客户阻断交易。

5.5 安全技术规范要求

5.5.1 客户端程序安全

5.5.1.1 客户端程序

5.5.1.1.1 基本要求

• 客户端程序上线前进行严格的代码安全测试。宁夏银行建立定期对客户端程序进行安全检测的机制。

• 客户端程序通过银行指定的第三方中立测试机构的安全检测，并出具检测报告。客户端程序具有抗逆向分析、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。

• 客户端程序的临时文件中没有出现敏感信息，临时文件包括但不限于 Cookies。客户端程序应禁止在身份认证结束后存储敏感信息，防止敏感信息的泄露。

• 客户端程序防范恶意程序获取或篡改敏感信息，例如使用浏览器接口保护控件进行防范。

5.5.1.1.2 增加要求

• 客户端程序保护在客户端启动的用于访问网上银行的进程，防止非法程序获取该进程的访问权限。

• 进行转账类交易时，客户端程序采取防范调试跟踪的措施，例如开启新的进程。

5.5.1.2 密码保护

5.5.1.2.1 基本要求

• 禁止明文显示密码，使用相同位数的同一特殊字符（例如*和#）代替。

• 密码应有复杂度的要求，包括：长度至少 6 位，支持字母和数字共同组成。

• 在客户设置密码时，提示客户不使用简单密码，不适用与其他网站相同或相似的密码。

• 如有初始密码，首次登录时强制客户修改初始密码，密码修改校验简单密码及特殊字符。

• 具有防范暴力破解静态密码的保护措施，例如在登录和交易时使用图形认证码，图形认证码应满足：由数字和字母组成；随机产生；包含足够的噪音干扰信息，避免恶意代码自动识别图片上的信息；具有使用时间限制并仅能使用一次。

• 使用软键盘方式输入密码时，对整体键盘布局进行随机干扰，同时具备防键盘记录、后台记录功能。。

• 保证密码的加密密钥的安全。

5.5.1.2.2 增加要求

• 采用辅助安全设备（例如 USB Key 或专用密码输入键盘）输入并保护密码。

• 密码输入后立即加密，敏感信息在应用层保持端到端加密，即保证数据在从源点到终点的过程中始终以密文形式存在。

• 密码输入框不允许 TAB 键跳转，也不允许快捷复制。

5.5.1.3 登录控制

5.5.1.3.1 基本要求

- 设置连续失败登录次数为 5 次以下，超过限定次数锁定网上银行登录权限。
- 退出登录或客户端程序、浏览器页面关闭后，立即终止会话，保证无法通过后退、直接
- 输入访问地址等方式重新进入登录后的网上银行页面。
- 退出登录时提示客户取下专用辅助安全设备，例如 USB Key。
- 每次登录回显客户上次登录时间、IP 地址及总登录次数。

5.5.1.3.2 增强要求

- 登录后超过一定时间未操作，自动断开与客户会话。

5.5.2 USBKey 安全要求

5.5.2.1 基本要求

- 使用符合国家安全标准，通过第三方中立测试机构安全检测通过的 USBKey。
- USBKey 采用具有密钥生成和数字签名运算能力的智能卡芯片，保证敏感操作在 USB Key 内进行。
- USBKey 的主文件（Master File）受到 COS 安全机制保护，保证客户无法对其进行删除和重建。
- 保证私钥在生成、存储和使用等阶段的安全。
- 参与密钥、PIN 码运算的随机数在 USBKey 内生成，其随机性指标符合国际通用标准的要求。
- 保证 PIN 码和密钥的安全：采用安全的方式存储和访问 PIN 码、密钥等敏感信息；PIN 码和密钥（除公钥外）不能以任何形式输出；经客户端输入进行验证的 PIN 码在其传输到 USB Key 的过程中，应加密传输，并保证在传输过程中能够防范重放攻击；PIN 码连续输错次数达到错误次数上限（不超过 10 次），USBKey 应锁定；同一型号 USB Key 在不同银行的网上银行系统中应用时，使用不同的根密钥，且主控密钥、维护密钥、传输密钥等对称算法密钥使用根密钥进行分散。

5.5.2.2 增强要求

- USBKey 能够防远程挟持，例如具有屏幕显示、语音提示、按键确认等功能，可对交易指令完整性进行校验、对交易指令合法性进行鉴别、对关键交易数据进行输入和确认。
- 未经按键确认，USBKey 不得签名和输出，在等待一段时间后，可自动清除数据，并复位状态。

5.5.3 安全认证

5.5.3.1 基本要求

- 网上银行服务器与客户端进行双向身份认证。
- 整个通讯期间，经过认证的通讯线路一直保持安全连接状态。
- 网上银行系统可判断客户的空闲状态，当空闲超过一定时间后，自动关闭当前连接，客户再次操作时必须重新登录。
- 确保客户获取的银行 Web 服务器的根证书真实有效，可采用的方法包括但不限于：在客户开通网上银行时分发根证书，或将根证书集成在客户端控件下载包中分发等。

5.5.3.2 增强要求

• 网上银行系统判断同一次登录后的所有操作必须使用同一 IP 地址和 MAC 地址，否则服务器端自动终止会话。

• 宁夏银行使用获得国家主管部门认定的具有电子认证服务许可证的 CA 证书及认证服务。

5.5.4 Web 安全

• 能够对系统的最大并发会话连接数进行限制。
• 能够对单个用户的多重并发会话进行限制。
• 能够对一个时间段内可能的并发会话连接数进行限制。
• 应用系统通信双方中的一方在指定时间内未作任何响应，另一方能够自动结束会话。
• 会话标识随机并且唯一。
• 会话过程中维持认证状态，防止客户通过直接输入登录后的地址访问登录后的页面。
• 转账交易后，确保使用浏览器的“后退”功能无法查看上一交易页面的重要客户信息。
• 网上银行系统 Web 服务器应用程序设置客户登录网上银行后的空闲时间，当超过指定时间，应自动终止会话。
• 禁止在 Web 应用程序错误提示中包含详细信息，不向客户显示调试信息。
• 禁止在 Web 应用服务器端保存客户敏感信息。
• 网上银行系统 Web 服务器应用程序应对客户提交的所有表单、参数进行有效的合法性判断和非法字符过滤，防止攻击者恶意构造 SQL 语句实施注入攻击。
• 数据库应尽量使用存储过程或参数化查询，并严格定义数据库用户的角色和权限。
• 通过严格限制客户端可提交的数据类型以及对提交的数据进行有效性检查等有效措施防止跨站脚本注入。
• 防范对网上银行服务器端的 DOS/DDOS 攻击。
• 主动监测钓鱼网站，及时发现，快速应对和处置。
• 主动监测 DNS 服务，发现异常及时预警，快速应对处置。
• 主动监测安全设备日志、网络流量、主机日志、应用日志，结合互联网威胁情报和资产脆弱性，利用大数据分析技术，运用人工智能算法，多维度分析，发现和预警网络攻击和业务异常行为，实时监控，快速应对处置。
• 定期主动开展漏洞扫描、互联网资产核查、渗透测试、业务安全评估、安全分析等安全评估工作，及时发现安全隐患，快速应对处置。
• 定期检查更新网络安全策略、安全设备检测特征库，发现和修复基础软硬件漏洞。

6 服务功能

本行网上银行服务系统包括个人网上银行系统、企业网上银行系统、银企直连以及网上银行业务管理平台。

个人网上银行系统可实现账户查询、交易明细查询、电子回单、网银日志查询、基金、理财、大额存单、定活互转、行内转账、跨行转账、批量转账、批量转账、定时汇款、超级网银、跨行收款签约、手机号汇款、预约信息管理、收款人名册管理、贷款查询还款，综合授信贷款资助发放、信用卡申请、还款、生活代缴费、客户服务等全流程金融服务功能。

企业网上银行系统可实现余额查询、保证金账户查询、账户明细查询、跨行转账查询、客户回单打印、开户行查询、行内转账、跨行转账、收款人名册管理、活期转定期、定期转活期、登录密码修改、常用功能设置、操作员日志查询、批量代发、跨行批量转账、电子银行承兑汇票、电子支付签约、业务复核等功能。

银企直联系统具备标准化接口，可直接与企业财务系统或资金平台无缝对接，通过企业平台实现本行网上银行提供的余额查询、行内转账、跨行转账、批量代发、批量跨行转账、自动归集、行名行号下载等定制化金融服务。

网上银行业务管理系统可实现网上银行服务系统日常业务管理功能。主要包括：包括企业开户、操作员管理、审核流程设置、落地限额设置，节假日维护、机构参数维护等运维功能。此外应能够提供细致的报表管理，包括交易量统计、签约客户统计、活动客户达标数、手续费收支情况、企业网上银行代发工资统计表等相关数据统计。

7 服务性能

本行网上银行引入业内知名开发公司进行规划及开发，搭建了业务迭代快速、功能齐备可拓展、安全可靠的网上银行服务体系，实现与行内资源业务整合输出、业务快速响应、业务处理安全、稳定等目标。

本行网上银行为客户提供一站式服务，扁平化的菜单展示，可根据客户喜好自行设置常用功能菜单等方式，同时在微信公众号、官网不定期发布新功能、新业务推介，帮助客户了解网上银行业务功能，提供客户满意度。

8 服务体验

8.1 客服人员行为规范

为不断提高我行客户服务质量，实行规范化客户服务管理体系，为本行客户提供安全、规范、高效的服务，本行制定了《客服中心管理章程》《客服中心业务处理流程》《客服中心服务规范话束》《客户投诉管理办法》《客服中心客户投诉应急预案》《客服中心服务应急预案》等制度，明确了客服人员行为规范、工作职责、服务规范、业务流程、服务应急流程、客户投诉及建议处理流程、处理时限和客户满意度回访等规范要求，并通过后续的质量监督、绩效考核及行为管理等方面进行全过程管理，保障服务质量和客户体验。

8.2 客服人员工作操守

要求客服人员严格遵守银行从业人员职责操守，遵守客户信息保密及本行所有规章制度，严格执行客服人员行为规范、设备使用规范、请示报告规范、上下班管理规范、请休假管理等相关规范，确保客服人员操守、行为、执行等符合规范管理要求。

8.3 客户服务规范

要求客服人员严格执行本行相关服务规范，做到业务熟练、语言规范、普通话标准、态度热情、语气柔和、耐心主动的解答客户业务咨询，解决客户问题。

8.4 柜面人员客户服务

客户在各营业网点办理网上银行签约业务，要求柜面人员主动向客户介绍网上银行签约业务流程及所需业务申请资料、协议签署规范及签约申请表填写规范和网上银行功能介绍，风险防范安全常识。大堂经理和客户经理要主动宣传网上银行业务服务功能、负责协助企业客户安装调试企业网上银行运行环境，安装必要插件，帮助客户解决日常使用当中存在的问题。

8.5 业务主管部门职责

网络金融部作为业务主管部门负责网上银行涉及客户投诉、建议的处理，协调相关部门、分支机构就客户投诉或建议事项提出处理意见或改进需求，并将处理情况及时反馈客户。

9 服务保障

9.1 组织保障

网上银行业务应遵循“统一管理、分级经营、保障安全”的原则。总行各条线管理部门按照统一管理、分级经营的原则，各机构严格履行工作职责，加强业务管理，规范业务操作，保障网上银行安全平稳运营，，积极开展网上银行业务营销、推广、经营活动。

9.1.1 网络金融部

作为全行网上银行业务的管理、牵头、实施部门，主要负责：
制定网上银行的业务计划和市场营销策略，组织开展网上银行的市场推广；
制定网上银行的业务管理制度并组织培训、检查督导和修订完善；
负责网上银行的业务需求统筹、界面设计和测试等工作；
负责网上银行服务价格的制定，处理网上银行业务投诉及建议；
执行监管机构和总行的反洗钱要求，开展网上银行反洗钱宣传，配合做好网上银行反洗钱工作；
按规进行业务审批、参数管理、后台维护、交易监测及其他与网上银行业务相关的工作；
制定电子银行业务连续性计划，保证电子银行业务的连续正常运营；
制定电子银行应急计划和突发事件处理预案，并定期对应急计划和预案进行演练，以管理、控制和减少意外事件造成的危害。

9.1.2 金融科技部

负责网上银行系统的技术研发、日常维护、信息安全、技术支持及其他与网上银行相关的技术性工作。制定技术安全管理策略、业务连续性应急预案及应急演练方案，及时解决网上银行系统运行中出现的技术问题；
协助网络金融部解决客户使用网上银行中遇到的问题，对网上银行运营以及安全控制设施设备采取适当的安全保护措施。

9.1.3 运营管理部

负责网上银行业务涉及会计核算的管理；
规范和管理全行柜面人员网上银行业务操作，汇总分支机构对于网上银行系统的业务需求，提出系统功能优化需求；

网上银行与综合业务系统对接的联调测试工作；

柜面 USB-Key 的日常管理工作。

9.1.4 审计部

负责对网上银行的安全管理进行稽核监督。

9.1.5 风险管理部

负责对网上银行业务连续性进行指导和管理，协助制定网上银行应急预案等。牵头组织开展网上银行业务风险状况的分析评价，对风险监控薄弱环节提出加强管理的意见。

9.1.6 各分支机构

负责网上银行柜面业务办理，包括客户申请资料审核保管、证书发放、落地业务处理和其他网上银行指定的业务；负责引导客户正确使用网上银行，并做好业务宣传、投诉建议处理和业务咨询等客户服务工作。

9.2 制度保障

为确保本行网上银行业务的正常开展，规范和完善网上银行业务管理，维护本行和客户的合法权益，本行先后制定了《宁夏银行电子银行章程》《宁夏银行网上银行业务管理办法》、《宁夏银行个人网银行业务操作规程》、《宁夏银行企业网银操作规程》、《宁夏银行网上银行业务运营中断突发事件专项应急预案》，下发了《宁夏银行网上银行业务操作规范》、《宁夏银行网上银行客户服务手册》、《宁夏银行网上银行版本更新说明》等操作文件，各分支机构须严格按照上述制度要求开展网上银行业务。

9.3 培训保障

按季度开展网上银行集中培训、业务推介和专项专题培训。针对网上银行系统开发的新业务、新产品，要先行出台相应的业务操作规程，并组织全行员工开展业务培训，并由本行员工先行试用后方可对外正式发布运营。

9.4 业务检查

网络金融部按季度对分支机构网上银行也进行检查，做到全年 100%网点全覆盖，针对检查出来的问题，问题反馈，做持续跟进，落实风控责任，改进网上银行产品质量。

9.5 客户隐私保护

严禁擅自将客户资料或我行内部资料外传，客户信息查询系统按机构设置权限，无法跨机构、模糊查询客户相关信息，系统内客户关键字段做屏蔽处理，相关查询信息也无法下载，尽可能保护客户隐私。