附件 8

ICS 35.240.40
CCS A 11

JR

中 华 人 民 共 和 国 金 融 行 业 标 准

JR/T 0231—2021

银行第三方软件开发工具包（SDK）安全接入指南

Guidelines for security access of importing third party software development kit in bank

2021－07－22 发布　　2021－07－22 实施

中国人民银行　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。

本文件由中国银行业协会提出。

本文件由全国金融标准化技术委员会（SAC/TC 180）归口。

本文件起草单位：中国银行业协会、中国工商银行股份有限公司、中国农业银行股份有限公司、中国银行股份有限公司、兴业银行股份有限公司、北京银联金卡科技有限公司、北京梆梆安全科技有限公司、北京奇虎科技有限公司、网神信息技术（北京）股份有限公司。

本文件主要起草人：潘光伟、张芳、高峰、李宽、王阳、敦宏程、苏建明、刘涌、叶红、蒋家堂、孟宪哲、金驰、戴心齐、马强、牟天宇、李亚敏、赵成刚、陈嘉、胡江海、谢振哲、高强裔、贝松涛、郭显杰、林宝晶。

引　言

随着银行网上应用功能的日益丰富，软件开发工具包（SDK,software development kit）越来越多地集成到了银行网络金融应用当中，在支持方便快捷开发的同时，也在金融信息安全等方面带来了一些隐患和问题。

银行应用系统中集成第三方软件开发工具包关系金融信息系统的稳定可靠,不安全的第三方软件开发工具包引入银行应用系统可能带来用户信息泄露、资产窃取等风险，需要对银行引进第三方软件开发工具包的过程进行约束，规范第三方软件开发工具包引进的安全性，促进第三方软件开发工具包在银行各类应用中集成的安全、健康发展。

银行第三方软件开发工具包（SDK）安全接入指南

1 范围

本文件提供了第三方软件开发工具包（以下简称第三方工具包）引入的总体原则、工具包分类以及安全技术指南。

本文件适用于银行引入第三方软件开发工具包的安全技术参考，也供保险、证券等其他金融行业参考。

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 35273—2020 信息安全技术 个人信息安全规范

GB/T 36328—2018 信息技术 软件资产管理 标识规范

JR/T 0068—2020 网上银行系统信息安全通用规范

JR/T 0171—2020 个人金融信息保护技术规范

3 术语和定义

JR/T 0068—2020和JR/T 0171—2020界定的以及下列术语和定义适用于本文件。

3.1

软件开发工具包 software development kit； SDK

基于特定软件包、软件框架、硬件平台、操作系统等建立应用软件时所使用的软件开发工具集合。

3.2

宿主应用 host application

引用工具包的应用。

3.3

支付敏感信息 payment sensitive information

影响网上银行安全的密码、密钥以及交易敏感数据。

注：密码包括转账密码、查询密码、登录密码、证书的PIN等，密钥包括但不限于用于确保通讯安全、报文完整性等的对称密钥、私钥等，交易敏感数据包括但不限于完整磁道信息、有效期、CVN、CVN2。

[来源：JR/T 0068—2020,3.4]

3.4

个人金融信息 personal financial information

金融机构通过提供金融产品和服务或其他渠道获取、加工和保存的个人信息。

注：包括账户信息、鉴别信息、金融交易信息、个人身份信息、财产信息、借贷信息及其他反应特定个人某些情况的信息。

[来源：JR/T 0171—2020,3.2]

4 缩略语

下列缩略语适用于本文件。

CVN：安全验证码（Card Verification Number）

CVN2：安全验证码2（Card Verification Number 2）

DNS：域名服务器（Domain Name System）

PIN：个人识别密码（Personal Identification Number）

SSL：加密套接字协议层（Secure Socket Layer）

TLS：安全传输层协议（Transport Layer Security）

UI：用户界面（User Interface）

WAP：无线应用协议（Wireless Application Protocol）

5 工具包分类

第三方工具包按照集成、工作方式，可分为以下类型：

a) 无交互类 SDK：SDK 完全嵌入到宿主应用中，SDK 服务的对象为银行应用的用户，SDK 不主动与第三方服务端交互，当 SDK 需要获取信息时，由宿主应用经由银行服务端向第三方服务端发起信息获取请求，第三方服务端反馈无差别的数据，框架见图 1。

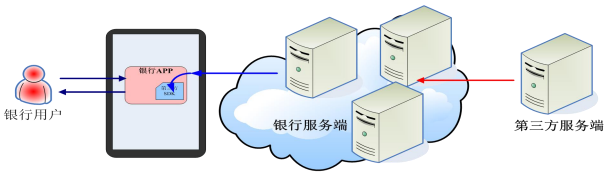

图 1 无交互类 SDK 框架示意图

b) 推送类 SDK：SDK 由嵌入到宿主应用部分和第三方服务端部分组成，SDK 服务的对象为宿主应用（银行应用）的用户，SDK 需要主动与第三方服务端进行通信，SDK 仅向第三方服务端发送简单参数信息（不包括能够定位到个体的个人金融信息或支付敏感信息），第三方服务端根据参数向 SDK 推送数据，框架见图 2。

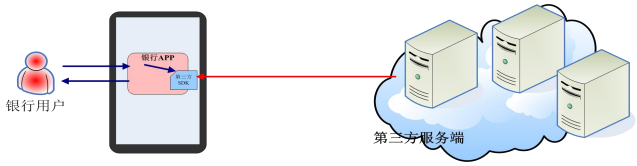

图 2 推送类 SDK 框架示意

c） 交互服务类 SDK：SDK 由嵌入到宿主应用部分和后台服务器部分组成，SDK 服务对象为宿主应用（银行应用）的用户和第三方应用的用户，工具包需要主动与后台服务器进行通信，工具包将用户输入信息反馈至后台服务器，通过交互实现功能，框架见图 3。

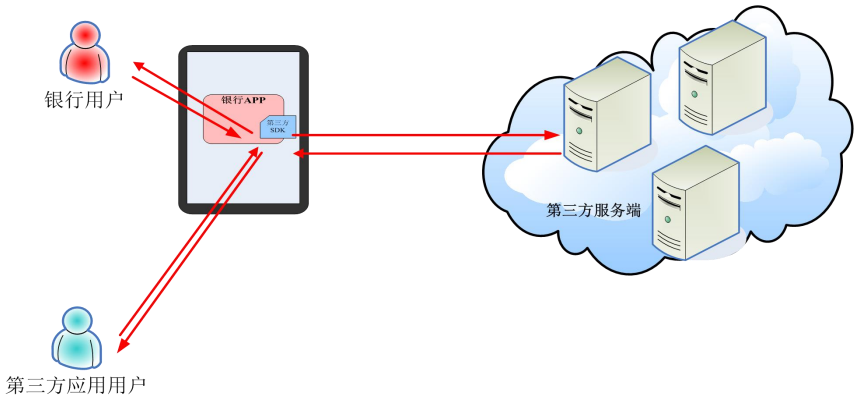

图 3　交互服务类 SDK 框架示意

SDK的安全设计宜符合JR/T 0068—2020的规定，同时对于不同类型的SDK，其安全接入存在差异的，在第7章中，将根据工具包类型给出差异化的安全规定。

6　总体原则

6.1　信息保护

第三方工具包在宿主应用中进行信息处理时在遵守GB/T 35273—2020中第6章规定的基础上，宜遵循以下原则：

a） 处理个人金融信息或支付敏感信息具有特定、明确、合理的目的，不扩大使用范围，在未声明情况下不改变处理敏感信息的目的。

b） 处理个人金融信息或支付敏感信息前，对敏感信息的获取目的、获取内容、使用范围、采用的防护措施等进行说明和告知。

c） 只处理与处理目的有关的最少信息，达到处理目的后，删除敏感信息。

d） 明确个人金融信息或支付敏感信息处理过程中的责任，采取相应的措施落实相关责任，并对敏感信息处理过程进行记录以便追溯。

e） 不超出授权范围获取交易数据、客户及客户端信息等内容。

f） 未经授权情况下，不向非相关方提供宿主应用接口、交易数据、客户及客户端信息等内容。

6.2　信息透明

第三方工具包的信息声明宜符合GB/T 36328—2018的规定。对于不符合的，宜提供以下信息：

a） 工具包名称及散列值。

b） 自身版本信息及兼容的宿主应用版本信息。

注：此处的宿主应用版本信息指银行移动应用版本信息。

c） 实现功能所需要的权限以及权限的使用条件。

d） 实现功能所需接触的敏感信息种类、操作类型、使用条件。

e） 引用的其他方组件信息。

f) 是否具有动态代码加载功能。
g) 工具包功能，包括但不限于推送、分享、计算、资源等。
h) 工具包集成、工作方式。

6.3 无主观恶意

第三方工具包不宜实现所声明功能以外的其他功能，不宜包含以下主观恶意行为：
a) 恶意扣费行为。
b) 隐私窃取行为。
c) 远程控制行为。
d) 恶意传播行为。
e) 资费消耗行为。
f) 系统破坏行为。
g) 诱骗欺诈行为。
h) 流氓行为。
各类主观恶意行为具体界定方式见附录A。

6.4 全周期管理

对第三方工具包的管理采取全周期管理原则，对合作方的接入前审核、引入中监控、退出时审计追溯等进行全周期管理。涉及第三方嵌入或接入的工具包，开展技术检测确保其个人信息收集、使用行为符合约定，并对收集个人金融信息或支付敏感信息的行为进行审计，发现超出约定的行为及时切断接入。

本文件正文部分给出了工具包的安全设计条件，可作为银行接入阶段的安全审核规范。银行在集成第三方工具包时的安全审核和运维条件见附录B。

7 第三方工具包设计安全

7.1 资源控制

不同类型的第三方工具包对宿主资源的调用宜满足表1的要求。

表 1 资源控制安全设计

安全设计	无交互类	推送类	交互类
不突破宿主应用限制并更改相关内容。	是	是	是
提供服务优先级设定功能，能够配合宿主应用实现根据优先级分配系统资源。	是	是	是
限制与外部数据源的最大会话连接数、单位时间会话建立数。	否	是	是
对软件开发工具包权限申请进行控制，采取最小授权原则，涉及用户个人信息处理的权限，单独向用户明示、申请。	否	否	是
对授权策略进行登记，并对软件开发工具包的敏感信息操作情况进行记录。	否	否	是

7.2 身份认证

不同类型的第三方工具包嵌入宿主部分与后台服务器部分间通信宜满足表2的要求。

表 2 身份认证安全设计

安全设计	无交互类	推送类	交互类
工具包不与后台服务器通信，需要进行数据更新时，通过宿主应用获取更新数据。	是	否	否
工具包嵌入宿主部分对后台服务器部分进行身份认证。	否	是	是
工具包嵌入宿主部分与后台服务器部分间的身份认证宜采用数字签名技术。	否	是	是
选取的身份认证、数字签名技术，符合 JR/T 0068—2020 中 6.2.2 的规定。	否	是	是

7.3 访问控制

不同类型的第三方工具包对宿主敏感信息取用以及工具包与后台服务器间交互宜满足表3的要求。

表 3 访问控制安全设计

安全设计	无交互类	推送类	交互类
对工具包权限申请进行控制，采取最小授权原则。	是	是	是
工具包嵌入宿主部分仅能接收限定的后台服务器推送的数据，宜通过宿主应用与后台服务器进行通信。	否	是	否
工具包嵌入宿主部分仅能与限定的后台服务器进行数据交互，采用固定互联网协议地址、域名、白名单等方式，防止 DNS 欺骗、流量劫持等攻击。	否	否	是
工具包后台服务器在非授权情况下不主动唤醒嵌入宿主部分。	否	是	是
传输会话加入超时机制。	否	否	是
工具包提供工具包的授权策略和敏感信息使用情况记录。	否	否	是

7.4 数据安全

不同类型的第三方工具包在遵守JR/T 0171—2020中第6章规定的基础上，还宜满足表4的要求。

表 4 数据安全相关安全设计

安全设计	无交互类	推送类	交互类
不收集、存储、转发宿主应用信息。	是	是	否
不存储用户个人信息，确需存储个人信息的，提前申请权限并对敏感信息进行加密保护。	否	否	是
对于提供的 UI 组件，提供安全保护措施，确保 UI 在进行用户交互时敏感信息不被泄露。当 SDK 或宿主处于前台，且 UI 展示特定敏感信息时，强制关闭系统截屏功能。	是	是	是
SDK 或宿主进入后台时，系统不保存当前屏幕。	是	是	是
SDK 需要能够确保敏感信息不会通过共享的系统资源被未授权的软件或进程获取。	是	是	是
同台设备多个宿主应用嵌入相同类型工具包，工具包不响应非本宿主的推送消息。	是	是	是
与后台服务端之间的数据传输使用加密保护措施，确保通信报文无法被拦截、篡改、伪造、重放，选取的加密保护措施符合 JR/T 0068—2020 中 6.2.2 的规定。	否	是	是
对页面展示数据采取适当的机密性保护措施。	是	是	是
工具包不收集、处理、存储个人金融信息、支付敏感信息，相关信息的输入、处理，宜在银行应用中进行。	否	否	是
除特别允许的情况外，不在 SDK 中硬编码存储敏感信息，如系统密钥等。	是	是	是

7.5 软件容错

不同类型的第三方工具包在软件容错方面宜满足表5的要求。

表 5　软件容错安全设计

安全设计	无交互类	推送类	交互类
提供保护功能，当嵌入宿主工具包发生故障时，不影响宿主应用功能。	是	是	是
对客户屏蔽技术错误信息，按双方预定规则，由开发包将产生的错误信息向宿主程序进行备案。	是	是	是
允许同台设备不同宿主嵌入相同的或同类型的工具包。	是	是	是
工具包后端服务器错误不导致嵌入宿主工具包崩溃。	否	是	是

7.6　攻击防护

不同类型的第三方工具包在针对外部攻击的检测、防护等方面宜满足表6的要求。

表 6　攻击防护安全设计

安全设计	无交互类	推送类	交互类
工具包中使用了其他第三方组件或中间件的，使用安全的第三方组件或中间件，对于开源的第三方组件或中间件，从可信途径获取并及时安装补丁，对于商业版本组件或中间件，使用授权版本。	是	是	是
能防止被动态调试。	是	是	是
能防止进程注入。	是	是	是
能防止被反编译。	是	是	是
能防止被篡改。	是	是	是
完整性校验无法被绕过。	是	是	是
后端服务器杜绝常见的漏洞。	否	是	是
具有重放检测功能。	否	是	是
具备抗抵赖机制。	否	是	是
安全键盘类工具包能对敏感信息进行及时加密，防止内存被转存。	否	是	是

7.7　安全审计

不同类型的第三方工具包安全审计方面宜满足表7的要求。

表 7　安全审计安全设计

安全设计	无交互类	推送类	交互类
工具包能够提供独立于宿主应用的安全审计日志记录功能。	是	是	是
审计日志包含工具包的操作类型、操作时间、操作结果等内容。	是	是	是
按照宿主应用需求上报安全审计日志。	是	是	是
安全审计日志不包含敏感信息。	是	是	是
后端服务器对与嵌入宿主工具包的数据通信行为进行记录，内容包括通信认证信息、通信起止时间、通信流量、是否传输敏感信息等。	否	是	是
工具包独立于宿主应用的安全审计日志，确保日志的有效性，涉及银行交易日志按照国家会计准则规定予以保存，系统日志保存期限不少于一年。	否	是	是

7.8　个人信息收集

第三方工具包收集个人信息宜满足以下条件：

a) 不欺诈、诱骗、强迫个人信息主体提供其个人信息。

b) 不隐瞒产品或服务所具有的收集个人信息的功能。

c) 不收集法律法规明令禁止收集的个人信息。

d) 收集的个人信息的类型与实现产品或服务的业务功能有直接关联。

注：直接关联是指没有该信息的参与，产品或服务的功能无法实现。

e) 工具包提供方将工具包需采集的个人信息、用途及采集频率告知银行。

f) 工具包提供方在声明中明确说明数据采集和使用的主体，并就信息获取行为取得客户的明示同意，内容包括工具包提供方收集、使用个人信息的规则。

注：如收集和使用个人信息的目的，收集方式和频率，存放地域，存储期限，自身的数据安全能力，对外共享、转让、公开披露的有关情况等。

7.9 第三方工具包交付

在第三方工具包交付方面宜满足以下条件：

a) 提供安全测试报告，测试报告检测内容包含本文件中安全设计中的全部内容。

b) 提供工具包集成手册，集成手册包含工具包的设计、功能、调用方法等内容。

c) 工具包提供方若发现银行应用、工具包自身、工具包集成组件存在安全缺陷，及时通知银行，未经银行许可，不将缺陷细节透露给任何其他第三方。

d) 工具包发生变更时，及时评估影响并告知银行，配合银行制定变更方案和应急预案。

e) 工具包提供方配合银行进行问题、事件分析。

附 录 A
（资料性）
第三方工具包恶意行为

A.1 概述

本附录提及的用户，均是使用了涉及到本附录所提及的软件开发工具包的银行移动应用办理银行业务，也即以银行移动应用程序为渠道使用银行产品服务的银行客户。

本附录提及的恶意行为，均是与银行和用户间就通过银行移动应用程序提供银行产品服务所必须的行为不符的行为，不论这些行为是否给用户带来了实际的损害。

A.2 恶意扣费行为

第三方工具包恶意扣费行为包括但不限于以下内容：

a) 在用户不知情或未授权的情况下，自动订购增值业务。
b) 在用户不知情或未授权的情况下，自动利用支付功能进行消费。
c) 在用户不知情或未授权的情况下，自动拨打收费声讯电话。
d) 在用户不知情或未授权的情况下，自动订购其他收费业务或扣除用户资费。

A.3 隐私窃取行为

第三方工具包隐私窃取行为包括但不限于以下内容：

a) 在用户不知情或未授权的情况下，获取终端设备信息。
b) 在用户不知情或未授权的情况下，获取用户个人信息。
c) 在用户不知情或未授权的情况下，利用终端信息采集设备获取音频、视频、图片信息。
d) 在用户不知情或未授权的情况下，获取其他非公开信息。

A.4 远程控制行为

第三方工具包远程控制行为包括但不限于以下内容：

a) 由控制端主动发出指令进行远程控制。
b) 由受控端主动向控制端请求指令。

A.5 恶意传播行为

第三方工具包恶意传播行为包括但不限于以下内容：

a) 自动发送包含恶意程序链接的短信、彩信、邮件、WAP 信息等。
b) 自动发送包含恶意程序的彩信、邮件等。
c) 自动利用无线通讯技术（包括蓝牙、红外、无线网络）向其他设备发送恶意程序。
d) 自动向移动存储设备上复制恶意程序。
e) 自动下载恶意程序。
f) 自动感染其他文件。

A.6 资费消耗行为

第三方工具包自费消耗行为包括但不限于以下内容：

a) 在用户不知情或未授权的情况下，自动拨打电话。
b) 在用户不知情或未授权的情况下，自动发送短信。
c) 在用户不知情或未授权的情况下，自动发送彩信。
d) 在用户不知情或未授权的情况下，自动发送邮件。
e) 在用户不知情或未授权的情况下，频繁连接网络，产生异常数据流量。

A.7 系统破坏行为

第三方工具包系统破坏行为包括但不限于以下内容：

a) 导致终端硬件无法正常工作。
b) 导致终端操作系统无法正常运行。
c) 导致终端其他非恶意软件无法正常运行。
d) 对系统文件或其他非恶意软件进行删除、卸载、终止进程或限制运行。

A.8 诱骗欺诈行为

第三方工具包诱骗欺诈行为包括但不限于以下内容：

a) 伪造、篡改、劫持信息，以诱骗用户，达到不正当目的。
b) 伪造、篡改用户文件或其他非恶意软件，以诱骗用户，达到不正当目的。
c) 冒充国家机关、金融机构、移动终端厂商、运营商或其他机构和个人，以诱骗用户，达到不正当目的。
d) 伪造事实，诱骗用户退出、关闭、卸载、禁用或限制使用其他合法产品或退订服务。

A.9 流氓行为

第三方工具包流氓行为包括但不限于以下内容：

a) 在用户不知情或未授权的情况下，长期驻留系统内存。
b) 在用户不知情或未授权的情况下，长期占用终端处理器计算资源。
c) 在用户不知情或未授权的情况下，自动捆绑安装。
d) 在用户不知情或未授权的情况下，自动添加、修改、删除收藏夹、快捷方式。
e) 在用户未授权的情况下，弹出广告窗口。
f) 用户无法正常退出程序。
g) 用户无法正常卸载、删除程序。
h) 在用户未授权的情况下，执行其他操作。

附 录 B
（资料性）
银行集成第三方软件开发工具包的安全指南

B.1 第三方工具包安全集成

B.1.1 工具包提供方核准

银行对工具包提供方进行审核，并制定以下相关合作协议：

a) 对工具包提供方进行接入审核，如从服务客群、服务场景、市场份额、运营能力、风险控制能力等方面进行考察。
b) 对于交互服务类工具包，全面审慎地考察工具包提供方的服务运行环境、评估其技术能力和管理水平，将用户信息保护能力作为重要评价指标，必要时对工具包提供方的安全保护能力进行技术评估。
c) 制定信息保护合作协议，对用户信息保密、交易安全等条款进行约定。
d) 对工具包提供方的相关资质进行核验，包括但不限于运营资质、法人信息材料。

B.1.2 安全传输

第三方工具包与服务器之间的数据传输宜符合以下安全设计要求：

a) 采用数字签名校验等手段，保证数据传输的完整性。
b) 采用 SSL 或 TLS 等安全通道连接进行通信，宜使用 TLS1.2 及以上版本。

B.1.3 运行安全

B.1.3.1 权限控制

银行应用权限控制宜满足以下安全设计要求：

a) 采用最小权限原则进行授权，对于未授权的资源禁止访问。
b) 对于涉及获取、使用、变更用户信息、账户、资金等功能的，SDK 提供方告知用户获取信息主体的情况下取得用户明示同意，其内容包含授权有效期。
c) 对工具包的接入有效期、权限有效期等进行控制（如单次有效、阶段性有效、协议期限内有效）。

B.1.3.2 数据安全

银行在使用第三方工具包时，数据安全保护方面宜满足以下安全设计要求：

a) 对数据完整性进行校验，并在检测到完整性错误时采取必要的恢复措施或停止执行请求。
b) 对于在工具包提供方服务端需要支付敏感信息或身份鉴别信息的场景，银行仅可作为信息的采集与传输通道，并采取报文加密等措施，保证采集与传输信息的机密性与完整性。
c) 使用数字签名等技术确保数据的不可抵赖性，采用的技术符合 JR/T 0068—2020 中 6.2.2 的规定。
d) 在合作终止后，依据约定的方式删除（或销毁）相关数据。

B.1.4 应用方退出

银行制定有序、可行的应用方退出机制，保障账户、资金、信息安全，充分履行用户告知义务。

应用方按照银行的需求，妥善处理其通过银行应用程序接口获取的用户信息与银行业务有关资料，并在双方协定的期限内承担后续保密责任。

B.2 安全运维

B.2.1 安全监测

B.2.1.1 运维监测

运维监测宜满足以下条件：

a) 银行建立第三方工具包监控相关管理机制，或将第三方工具包监测纳入银行统一监测平台并重点监测。

b) 运维监测宜包含以下内容：

1) 监控第三方工具包后台相关服务器运行状态并建立告警机制。

2) 监控第三方工具包服务状态（包括耗时、交易量、成功率等参数）并建立告警机制。

3) 按照国家会计准则的规定，保存银行交易日志，保存期限不少于一年。

B.2.1.2 异常监测

异常监测宜满足以下条件：

a) 具备流量控制能力，控制措施包括告警、暂停、拒绝等。

b) 建立冒用第三方工具包服务端的监测机制，发现问题及时处置。

c) 具备故障监测和恢复能力。

B.2.2 工具包终止与系统下线

银行宜制定完善的第三方工具包服务终止和系统下线的相关制度和步骤，具体如下：

a) 第三方工具包服务终止时，银行将服务终止有关事项提前告知相关方。

b) 服务终止后，需将相关数据归档、数据删除（或销毁）、个人金融信息保护、用户资金和账户安全、消费者权益保护等问题与个人信息所有者充分达成一致，明确相关责任，并充分履行用户告知义务。

c) 系统下线在相关服务确认终止之后执行，在下线之前设置过渡期，并在应用中配置业务功能挡板，同时对用户进行提示，明示应用方服务已终止。

d) 银行在系统下线之后将有关数据进行归档处理，数据保留期限按照国家与行业主管部门、银行相关规定与规则执行。

参 考 文 献

[1] GB/T 25069—2010 信息安全技术 术语
[2] GB/T 35273—2020 信息安全技术 个人信息安全规范
[3] GB/T 36328—2018 信息技术 软件资产管理 标识规范
[4] JR/T 0068—2020 网上银行系统信息安全通用规范
[5] JR/T 0171—2020 个人金融信息保护技术规范