ICS 03.060
CCS A11

团 体 技 术 报 告

TR/CBA 214—2021

银行函证服务平台 运营规则

Banking confirmation service platform — rules of operation

2021－12－18 发布　　2021－12－18 实施

中国银行业协会　　发 布

目　　次

前　言

中国银行业协会(China Banking Association，CBA)成立于2000年5月，是经中国人民银行和民政部批准成立，并在民政部登记注册的全国性非营利社会团体，是中国银行业自律组织。2003年中国银监会成立后，中国银行业协会主管单位由中国人民银行变更为中国银监会。2018年3月，中国银行保险监督管理委员会成立后，中国银行业协会主管单位由中国银监会变更为中国银行保险监督管理委员会。凡经业务主管单位批准设立的、具有独立法人资格的银行业金融机构(含在华外资银行业金融机构)和经相关监管机构批准、具有独立法人资格、在民政部门登记注册的各省(自治区、直辖市、计划单列市)银行业协会以及相关监管机构批准设立，具有独立法人资格的依法与银行业金融机构开展相关业务合作的其他类型金融机构，以及银行业专业服务机构均能申请加入中国银行业协会成为会员单位。

中国银行业协会日常办事机构为秘书处。秘书处设秘书长1名，副秘书长若干名。根据工作需要，中国银行业协会设立32个专业委员会，其中银行业产品和服务标准化专业委员会旨在开展银行业产品和服务标准化工作，包括制定和发布银行业的产品和服务标准，积极参与制定国家标准、行业规划，参与制定有关政策和法律法规，不断提高银行业产品和服务质量。

本文件按照T/CBA 1—2021《中国银行业协会团体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这些专利的责任。

T/CBA 211—2021《银行函证服务平台 运营规则》是按照财政部和银保监会的要求构建的银行函证服务平台的工作技术依据系列文件之一，本系列文件结构如下：

——T/CBA 210—2021《银行函证服务平台 接入要求》；

——T/CBA 211—2021《银行函证服务平台 加密体系》；

——T/CBA 212《银行函证服务平台 基础数据元》；

——TR/CBA 213《银行函证服务平台 服务接口》；

——TR/CBA 214《银行函证服务平台 运营规则》。

本文件由中国银行业协会银行函证服务平台服务中心提出。

本文件由中国银行业协会银行业产品和服务标准化专业委员会归口。

本文件起草单位：中国银行业协会、工银科技股份有限公司、中国工商银行股份有限公司、中国农业银行股份有限公司、国家开发银行、广发银行股份有限公司、渤海银行股份有限公司、上海浦东发展银行股份有限公司、湖南三湘银行股份有限公司、沧州银行股份有限公司。

本文件主要起草人：潘光伟、刘峰、张亮、艾亚萍、高峰、李朋乐、李宽、张贺、赵世博、仲峻锋、王昭允、田丰、李新、沈建宾、郝佳、董健、倪晨、严彪、谢经纬、张福胜、丁明皓。

地 址：北京市西城区金融街 20 号交通银行大厦 B 座 11-12 层
电 话：010-66553368 010-66291132
邮 编：100033
邮 箱：cba.china@china-cba.net
传 真：010-66553356

引　言

银行函证系统是实现银行函证业务数字化转型的重要技术支撑。为使银行函证系统的运作规范有序、有据可依，维护金融业机构和会计师事务所以及其他组织、机构的合法权益，促进银行函证业务的健康发展，根据《财政部 中国银保监会关于进一步规范银行函证及回函工作的通知》（财会〔2020〕12号）和有关监管要求，制定本文件。

本文件给出了银行函证服务平台的运营管理机构和银行函证服务平台的接入机构在函证业务运营过程中的相关规则，这些规则将按照银行函证服务平台的运营管理机构和银行函证服务平台的接入机构内部的管理体系和管理惯例，反映在其内控控制的相关文件中。

通过实施本文件，配套以相关的技术措施，能达到确保银行函证规范有序运行的目的。

银行函证服务平台 运营规则

1 范围

本文件给出了银行函证系统在运营过程中，银行函证服务平台的运营管理机构和银行函证服务平台的接入机构遵循的相关规则。

本文件适用于构成银行函证系统的银行函证服务平台运营单位、银行业金融机构、会计师事务所和相关机构。

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。

JR/T 0234—2021 数字函证金融应用安全规范

T/CBA 210 银行函证服务平台 接入要求

T/CBA 211 银行函证服务平台 加密体系

3 术语、定义和缩略语

下列术语和定义适用于本文件。

3.1

银行函证业务 banking confirmation business

会计师事务所等在获取被审计单位授权后，直接向银行业金融机构发出询证函，银行业金融机构针对所收到的询证函，查询、核对相关信息并直接提供回函的过程。

术语条目注 1：询证函可能是能够进行数据元解析的，也可能仅是一个图像或不可更改格式的文件。

术语条目注 2：《关于进一步规范银行函证及回函工作的通知》（财会〔2020〕12 号）中，界定的相关概念为“银行函证及回函，是注册会计师在获取被审计单位授权后，直接向银行业金融机构发出询证函，银行业金融机构针对所收到的询证函，查询、核对相关信息并直接提供书面回函的过程”。因本文件面向的实施对象不是注册会计师个人，而是会计师事务所，故对定义进行了调整。

[来源：T/CBA 210—2021，3.1，有修改——增加了术语条目注2]

3.2

银行函证系统 banking confirmation business system

处理银行函证业务的应用系统。

术语条目注 1：银行函证系统由银行函证服务平台、银行业金融机构、会计师事务所和相关机构构成，其框架和基本工作过程见 T/CBA 210—2021。

3.3

银行函证服务平台运营机构 managing organization for banking confirmation servicing platform

平台管理方

负责构建、运行银行函证服务平台以为银行函证系统（3.2）提供核心支撑并向银行函证服务平台接入机构（3.4）提供服务的机构。

3.4

银行函证服务平台接入机构 accessing organization for banking confirmation servicing platform

平台接入方

作为银行函证系统（3.2）的组成单元，接受银行函证服务平台运营机构（3.3）所提供服务的机构。

术语条目注 1：银行业金融机构、会计师事务所和相关机构均视作平台接入方。

4 平台接入准备

4.1 身份认证审核

平台管理方对计划接入平台的平台接入方进行线下审核及身份认证。平台接入方提交的材料包括：

a) 盖有平台接入方公章的接入银行函证服务平台申请表；

b) 平台接入方法定代表人签字或并盖有平台接入方公章的法人授权书；

c) 经办人居民身份证复印件，由平台管理方对法人授权书中被授权人（即经办人）进行身份信息实名认证；

d) 盖有平台接入方公章的营业执照复印件。

平台接入方提供上述资料不完整或有误的，平台管理方不得为其提供银行函证服务平台接入服务或终止已经提供的服务。

4.2 签订服务协议

平台管理方与平台接入方签署合作意向书和服务协议，由双方法定代表人签字并盖有双方公章，双方各存留两份。其中：

a) 合作意向书在启动阶段签署；

b) 服务协议在投产向公众提供服务之前签署。

合作意向书和服务协议的主要内容参见附录A。

4.3 平台接入要求

平台管理方与平台接入方根据业务需求和基础条件，列出实施T/CBA 210所规定的接入要求涉及到的相关工作、时间安排、实施人员和验收方法等。

5 平台对接开发

5.1 概述

仅应用系统接入方式涉及到平台对接开发，浏览器方式接入无需此过程。

T/CBA 210有规定的，按照T/CBA 210中的相关条款实施。

5.2 技术资源提供

平台管理方向平台接入方提供如下技术资源：

a) 技术对接手册；

b) 用户手册；
c) SDK 开发工具包；
d) 其他必要资源。

5.3 自行开发要求

应用系统由平台接入方自行开发的，符合如下要求：
a) 将开发环境与实际运行环境物理分开，使测试数据、测试过程和测试结果受到控制；
b) 制定软件开发管理制度，规范开发过程和人员行为；
c) 制定代码编写安全规范，要求开发人员参照规范编写代码；
d) 符合银行函证服务平台系列标准中涉及到接口的相关要求；
e) 具备软件设计的相关文档和使用指南，并对文档使用进行控制；
f) 保证在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测；
g) 对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制；
h) 保证开发人员为专职人员，开发人员的开发活动受到控制、监视和审查。

5.4 外包开发要求

应用系统由平台接入方外包给第三方开发的，除满足5.3的全部要求外，还应符合如下要求：
a) 在软件交付前检测其中可能存在的恶意代码；
b) 保证开发机构提供软件设计文档和使用指南；
c) 保证开发机构提供软件源代码，并审查软件中可能存在的后门和隐蔽信道；
d) 在软件交付前不提供生产密钥、银行函证服务平台的生产实际地址等关键信息给外包公司。

6 联调测试

6.1 概述

仅应用系统接入方式涉及到联调测试，浏览器方式接入无需此过程。
T/CBA 210有规定的，按照T/CBA 210中的相关条款实施。

6.2 技术准备

平台管理方与平台接入方进行如下技术准备：
a) 平台接入方提供测试环境系统配置文件，将测试环境公钥和区块链证书提供给平台管理方；平台接入方使用 OPENSSL 工具生成测试环境区块链证书，将区块链证书、制作区块链证书时的根证书 CN 参数值和子证书 CN 参数值提供给平台管理方；
b) 平台接入方提供测试环境防火墙，完成开通并验证；
c) 平台接入方与银行函证服务平台，双向开通防火墙；
d) 平台接入方为银行业金融机构的，提供各接口 URL 地址；
e) 平台接入方为银行业金融机构的，提供用于联调测试的被审计企业信息及测试数据，无需真实信息。

7 接入投产

平台接入方向平台管理方提供如下材料：

a） 生产环境接入申请表；
b） 采用应用系统接入方式接入的，联调测试报告；
c） 平台接入方生产环境系统配置文件；
d） 平台接入方生产环境公钥和区块链证书；
e） 采用应用系统接入方式接入的，生产环境防火墙开通验证报告，其中银行业金融机构至银行函证服务平台的防火墙双向开通；
f） 银行业金融机构采用应用系统接入方式接入的，各接口 URL 地址；
g） 会计师事务所提供用于投产验证的被审计企业信息及数据；
h） 平台接入方试运行方案；
i） 银行业金融机构的银行函证业务规则；
j） 银行业金融机构采用应用系统接入方式接入的，提供企业授权和缴费操作手册；
k） 会计师事务所提供其在指定银行开立对公账户的客户编号（用于指定银行设置白名单）。

平台管理方对上述材料进行审核与验证，验证通过后，完成投产准备工作。

8 业务过程

银行函证系统运营过程中遵守如下业务规则：

a） 会计师事务所必须按照财会〔2020〕12 号的要求，按照中国注册会计师审计准则的规定实施函证程序；
b） 在所有银行函证业务办理过程中，按照 T/CBA 211 的要求进行加密和解密。其中会计师事务所发送格式一以及验资业务函证申请前，使用平台提供的 SDK 加解密工具或国密算法，对申请文件加密后再向平台发送函证申请；由于格式二函证申请中不包含有商业机密信息，发送格式二函证申请前无需进行加密；
c） 被审计机构授权方式遵循 JR/T 0234—2021 中 6.2.3.6 的要求；
d） 当函证停留在“待授权”状态 3 个工作日后仍未通过授权，银行函证服务平台会向会计师事务所发送提醒邮件，会计师事务所要联系被审计机构进行授权；

注：银行函证系统业务流程请参考 T/CBA 210—2021 附录 A，银行函证服务平台的状态代码请参考 T/CBA 210—2021 附录 B。

e） 银行业金融机构因询证函不符合规定拒绝回函，要在收到被审计机构授权同意函证业务的 3 个工作日内通知会计师事务所，否则视同询证函符合规定；
f） 当函证停留在“待处理”状态（即函证授权通过后）7 个工作日后仍未回函，银行函证服务平台会向银行业金融机构发送提醒邮件督促回函；

注：银行函证系统业务流程请参考 T/CBA 210—2021 附录 A，银行函证服务平台的状态代码请参考 T/CBA 210—2021 附录 B。

g） 回函文件在银行函证服务平台存放 10 个工作日，10 个工作日后自动销毁。回函文件一旦被销毁是不可逆的，需要事务所重新发起新的函证。回函文件被销毁前 1 个工作日，银行函证服务平台向会计师事务所发送提醒邮件督促下载文件。

9 内部管控

9.1 平台接入方内部管控

平台接入方确立银行函证内部的管控要求，包括：

a） 统一牵头、分工负责的内部治理机制；
b） 与本机构治理架构一致的工作流程；
c） 所使用计算机的全生命周期的实体安全、信息安全与健康监控；
d） 银行函证服务平台用户的设定、变更；
e） 数字公钥的介质与应用口令的设定、变更、备份；
f） 函证文件产生、传递、存档；
g） 平台接入方私钥管控；
h） 可核查日志的生成、内容选择、日志记录内容的变更权限与流程、日志审计、日志存档；
平台接入方确立的规章制度和技术标准按照约定的方式使平台管理方知悉。

9.2 平台管理方内部管控

平台管理方确立银行函证内部的管理要求，包括：
a） 统一牵头、分工负责的内部治理机制；
b） 与本机构治理架构一致的工作流程；
c） 银行函证服务平台管理员用户的设定、变更；
d） 可核查日志的生成、内容选择、日志记录内容的变更权限与流程、日志审计、日志存档。

10 隐私保护

银行函证服务平台在运营过程中，实施如下隐私保护措施。
a） 注册信息。管控方式如下：
1） 浏览器方式接入的平台接入方需先由银行函证服务平台完成用户注册及创建。在创建过程中，用户需要提供机构基本信息、营业执照、法人授权书、经办人身份信息，以及对接人员、管理人员个人信息。平台使用这些信息从而授予接入方对平台服务的访问权；
2） 浏览器方式接入的平台接入方用户创建成功后，银行函证服务平台会向用户提交材料时预留的管理员邮箱发送一封电子邮件，通知该管理员已经开通了用户，并提供登录平台的初始密码。该电子邮件只用于提供平台服务，不用于任何其他目的。
b） 函证申请信息。管控方式如下：
1） 银行函证服务平台在会计师事务所用户提出函证申请时，银行函证服务平台要求会计师事务所用户提供被审计机构的相关信息（如被审计机构联系人姓名、手机号、电子邮件，被审计机构地址）和被审计机构银行账号等财务信息；
2） 上述信息用于填写函证申请、授权和缴费目的。如果银行函证服务平台在函证业务流转时遇到障碍，银行函证服务平台会使用这些信息来联系被审计机构。
c） 日志文件。管控方式如下：
1） 银行函证服务平台的日志文件记录了互联网协议（IP）地址、浏览器类型、互联网服务提供商（ISP）、登录/退出页面、操作系统和访问时间；
2） 银行函证服务平台仅使用日志文件来跟踪系统中的错误。日志文件信息不与用户的个人数据绑定。
d） Cookie 及相关技术使用。管控方式如下：
1） 银行函证服务平台的某些服务只能通过使用 Cookie 实现，银行函证服务平台可能通过放置安全的 Cookie 及相关技术收集用户的计算机浏览器信息；
2） 如用户的浏览器或浏览器附加服务允许，用户能够修改对 Cookie 的接受程度或者拒绝平台的 Cookie；

3) 如果停用 Cookie，用户可能无法享受最佳的服务体验，部分服务也可能无法正常使用。

e) 银行函证服务平台存储信息。管控方式如下：

1) 银行函证服务平台在中华人民共和国境内收集和产生的个人信息将存储在中华人民共和国境内；

2) 在用户终止使用银行函证服务平台服务后，银行函证服务平台会停止对用户的信息的收集和使用，法律法规或监管部门另有规定的除外；

3) 如银行函证服务平台停止运营，银行函证服务平台将及时停止收集用户数据信息的活动，将停止运营的通知以逐一电邮送达或消息公告的形式通知用户，并对所持有的用户的数据信息进行删除或匿名化处理。

f) 银行函证服务平台使用收集的信息。管控方式如下：

1) 银行函证服务平台收集的信息用于以下用途：

(1) 向用户提供服务，满足用户的个性化需求；

(2) 安全保障，用于身份验证、安全防范、反诈骗监测、存档备份、客户的安全服务等用途；

(3) 邀请用户参与有关平台服务的调查；

(4) 为了确保服务的安全，帮助平台更好地了解平台的运行情况，平台可能记录相关信息，例如，用户使用平台的频率、故障信息、总体使用情况以及性能数据等。

2) 若平台超出上述用途使用用户的信息，平台将再次向用户进行说明，并征得用户的同意。

g) 银行函证服务平台对外提供信息。管控方式如下：

1) 请求监管部门对用户的信息采取保护措施；

2) 在函证申请、回函业务中向用户相对方提供姓名、手机号、电子邮箱等信息，用于函证及回函业务所必需的沟通与联系；

3) 在函证业务查询中提供有关联系人（或操作人员）个人信息；

4) 以下情形中，平台可能会共享、查询数据信息且无需事先征得数据信息主体的授权同意：

(1) 与函证业务有关法律法规规定必须共享和/或提供的；

(2) 与国家安全、国防安全有关法律法规规定必须共享和/或提供的；

(3) 与公共安全、公共卫生、重大公共利益有关法律法规规定必须共享和/或提供的；

(4) 与刑事侦查、起诉、审判和判决执行等有关法律法规规定必须共享和/或提供的；

(5) 出于维护数据信息主体或其他个人的生命、财产等重大合法权益但又很难得到数据信息主体授权同意的；

(6) 从合法公开披露的信息中收集数据信息的，如合法的新闻报道、政府信息公开等渠道。

h) 用户访问和管理自己的信息。管控方式如下：

1) 用户能够在使用银行函证服务平台服务的过程中，访问用户提供的数据信息，也能够联系平台帮用户修改和删除数据信息；

(1) 用户能够查看用户预留的有关身份证号、手机号、电子邮箱等信息；为了用户的数据信息安全，将对有关身份证号码进行脱敏展示；

(2) 如用户发现银行函证服务平台违反法律、行政法规的规定或者双方的约定收集、使用用户的数据信息，用户能够要求银行函证服务平台删除；如用户发现银行函证服务平台收集、存储的用户的数据信息有错误的，用户也能够要求银行函证服务平台更正。

2) 银行函证服务平台必须执行相关法律法规和监管要求，在以下情形中，可能无法响应用户的请求：

(1) 与国家安全、国防安全直接相关的；

(2) 与公共安全、公共卫生、重大公共利益直接相关的；

(3) 与犯罪侦查、起诉、审判和执行判决等直接相关的；
(4) 有充分证据表明用户存在主观恶意或滥用权利的；
(5) 响应用户的请求将导致其他个人、组织的合法权益受到严重损害的；
(6) 涉及商业秘密的。

i) 涉及到业务相关场景中非自身接入方的隐私保护。管控方式如下：
1) 业务相关场景中用户的非自身接入方可能有自己的隐私权保护政策，非自身接入方对数据的使用可能未能通过相关文件得到与银行函证服务平台一致的约束；
2) 银行函证服务平台会尽商业上的合理努力去要求这些主体对用户的数据信息采取保护措施，但银行函证服务平台无法保证这些主体一定会按照平台的要求采取保护措施，必要时用户要与他们直接联系以获得关于他们的隐私权政策的详细情况；
3) 如用户发现非自身接入方开发的应用程序存在风险时，用户终止相关操作以保护用户的合法权益。

j) 银行函证服务平台的信息安全。管控方式如下：
1) 银行函证服务平台将持续优化以提供相应的安全保障，防止信息的丢失、不当使用、未经授权访问或披露；
2) 银行函证服务平台将在合理的安全水平内，使用诸如 HTTPS、SM4、SM2 等技术手段，以保障信息的安全；
3) 银行函证服务平台严格限制访问信息的人员范围，并进行相应的审计；
4) 若发生数据信息泄露等安全事件，银行函证服务平台会启动应急预案，阻止安全事件扩大，并以电话、短信或电子邮件等形式告知用户。

11 运维安全措施

11.1 平台接入方的运维安全措施

平台接入方采取如下措施：

a) 平台接入方制定运维安全规则，包括但不限于安全策略、用户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面规定；
b) 平台接入方按照对数据生命周期保护的安全要求，以数据分级为基础，建立覆盖数据生命周期全过程的安全防护体系，并通过建立健全数据安全组织架构和明确信息系统运维环节中的数据安全需求，全面保障金融机构数据安全；
c) 平台接入方不得将含有病毒的附件进行上传，危及平台安全；
d) 平台接入方如果出现机构信息、接入方式、机构公钥、区块链证书、机构状态、支持函证格式变更的情况，或出现机构管理员的人员变更、姓名或手机号信息、状态发生变更的情况，或发生机构管理员忘记登陆密码的情况，机构业务负责人使用工作邮箱发送变更申请至平台管理方系统管理员邮箱进行相应变更。

11.2 平台管理方的运维安全措施

平台管理方采取如下措施：

a) 平台管理方制定运维安全规则，包括但不限于安全策略、用户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面规定；

b) 平台管理方按照对数据生命周期保护的安全要求，以数据分级为基础，建立覆盖数据生命周期全过程的安全防护体系，并通过建立健全数据安全组织架构和明确信息系统运维环节中的数据安全需求，全面保障金融机构数据安全。

12 银行函证系统版本控制

12.1 银行函证服务平台

银行函证服务平台的版本控制与更新策略如下：

a) 银行函证服务平台以季度为周期收集迭代需求。在投产变更前 10 个工作日，根据迭代需求制定投产变更方案，上报给平台管理方负责人进行审批后实施；平台管理方在内部建立对系统变更的申报和审批控制程序，依据变更流程控制所有的变更。

b) 银行函证服务平台变更方案不涉及接入机构改造的，如停机时间不超过 0.5 小时的，不通知接入机构；如停机时间在 0.5-4 小时以内的，提前 5 个工作日通过电子邮件通知到各接入机构业务联系人与负责人；停机大于 4 个小时，提前 10 个工作日通过电子邮件通知到各接入机构业务联系人与负责人；涉及接入机构同步改造的，平台管理方与平台接入方协商共同开展开发、测试计划，协商投产变更时间计划后，同步发布上线。

12.2 接入的应用系统

平台接入方与银行函证服务平台连接的应用系统的版本控制与更新策略如下。

a) 平台接入方如在工作日日间（6:00-24:00）进行系统变更或停机维护，提前 3 个工作日向平台管理方提出变更计划，如需中断服务在 0.5 小时以上，平台管理方将进行公示；平台接入方如在工作日夜间（00:00-6:00）、非工作日或节假日进行系统变更或停机维护，提前 2 个工作日向平台管理方提出变更计划，如需中断服务在 2 小时以上，平台管理方将进行公示。

b) 提供变更申请包含但不局限于下列内容：

1) 变更请求的发起者；
2) 变更的目的和意义；
3) 变更的紧迫性和重要性（变更级别）；
4) 变更请求需要的答复响应时间；
5) 变更涉及的业务系统范围；
6) 变更对当前系统的影响；
7) 变更请求涉及和需要的各类资源，包括所必需的各类人力资源和物力资源；
8) 变更的必要性与可行性分析；
9) 变更的负责人及联系方式；
10) 详细的变更实施计划，包括但不限于变更实施步骤、回退步骤、紧急情况应对措施等内容；
11) 对变更结果的预测与评估；
12) 如为计划外变更（如临时紧急变更）或计划外停机（如系统服务异常）等情况，平台接入方应立即通知平台管理方，并事后补充相关报告。

13 函证服务系统应急管理

13.1 银行函证服务平台应急通报

银行函证服务平台针对高峰期和非高峰期分别提供针对性响应机制。银行函证业务高峰期通常是指每年1月至3月，可根据业务实际情况进行调整。

a) 业务高峰期：
   1) 故障响应支持。在服务期内发生日常故障且无法通过远程技术支持进行解决时，提供技术支持服务，2 小时之内响应，不影响系统运行的故障 72 小时内解决问题；影响系统运行的故障立即响应，通过电子邮件方式通知各接入机构，并在 4 小时内解决问题；
   2) 远程技术支持。在服务期内提供 5*8 小时电话、网络等热线技术支持服务，响应时间为 2 小时。
b) 非业务高峰期
   1) 故障响应支持。在服务期内发生日常故障且无法通过远程技术支持进行解决时，提供技术支持服务，4 小时之内响应，不影响系统运行的故障 96 小时内解决问题；影响系统运行的故障立即响应，并在 8 小时内解决问题；
   2) 远程技术支持。在服务期内提供 5*8 小时电话、网络等热线技术支持服务，通过电子邮件方式通知各接入机构，响应时间为 4 小时。

13.2 平台接入方应急通报与故障解决

平台接入方的应急通报与故障解决为：

a) 平台接入方在服务期内发生日常故障时，不影响系统运行的故障，在 72 小时内解决问题；
b) 影响系统运行的故障立即响应，第一时间通知平台管理方，并在解决问题后邮件通知平台管理方，说明停止服务的时间点和恢复服务的时间点。

附 录 A
（资料性）
合作意向书和服务协议的主要内容

A.1 合作意向书

合作意向书主要包括如下内容：

a) 平台接入方的资格声明；
b) 平台管理方的资格声明；
c) 双方合作基础和原则；
d) 涉及到法律法规和监管要求时双方分别的职责；
e) 支撑双方合作的信息系统的约定；
f) 平台接入方在准备接入银行函证服务平台过程中双方的职责；
g) 银行函证系统在运行过程中双方的职责；
h) 双方共同对通过银行函证系统办理银行函证业务的职责；
i) 双方对网络安全和数据安全的约定；
j) 双方在涉及到商业秘密时的处理约定；
k) 双方的知识产权约定；
l) 异议处理约定；
m) 合作变更与终止的约定；
n) 纠纷处理约定。

A.2 服务协议

服务协议主要包括如下内容。

a) 平台接入方的资格声明；
b) 平台管理方的资格声明；
c) 双方合作基础和原则；
d) 服务涉及到对象和相关支撑信息技术平台概念界定；
e) 服务内容，包括
    1) 服务前提；
    2) 应用场景；
    3) 接入方式；
    4) 推广与交流。
f) 权力与义务
    1) 权力与义务的描述；
    2) 超越权力和违反业务的罚则。
g) 协议生效与变更；
h) 服务费用与支付方式；

i） 保密要求；

j） 通知方式与送达约定。

参 考 文 献

[1] GB/T 20158—2006 信息技术 软件生存周期过程 配置管理
[2] GB/T 31595—2015 公共安全 业务连续性管理体系 指南
[3] GB/T 30146—2013 公共安全 业务连续性管理体系 要求