ICS 35.240.99
CCS L 77

团　　体　　标　　准

T/ISC 0016—2022

基于区块链的机构电子签约系统要求

Service specification for institutional e-signing based on blockchain

2022－08－05 发布　　2022－11－05 实施

中　国　互　联　网　协　会　　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这些专利的责任。

本文件由中国互联网协会提出并归口。

本文件主要起草单位：中国信息通信研究院，蚂蚁科技集团股份有限公司，微易签（杭州）科技有限公司，恒生电子股份有限公司，天翼电子商务有限公司，远光软件股份有限公司，杭州趣链科技有限公司，福建博思软件股份有限公司，平安国际智慧城市科技股份有限公司，联动优势科技有限公司

本文件主要起草人：张奕卉，庞伟伟，康宸，张启，程阳，童正，常帅，刘晓莹，肖承欣，彭晋，王昕，昌文婷，陈童，刘哲，李振，青龙生，占腾飞，张一博，贺伟，史楠迪，鲁静，李伟，张璐，杜静漪，李保丰，林承，姜德峰，陈正。

基于区块链的机构电子签约系统要求

1 范围

本文件确立了机构之间基于区块链技术的电子签约系统架构，描述了其业务流程，规定了其功能要求和安全要求。

本文件适用于机构之间的电子签约服务提供者规范业务活动，也适用于主管监管部门、第三方评估机构对机构电子签约业务进行监督、管理、评估时参考。

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 33190—2016 电子文件存储与交换格式 板式文档

GB/T 36298—2018 电子合同订立流程规范

GB/T 36319—2018 电子合同基础信息描述规范

GB/T 36320—2018 第三方电子合同服务平台功能建设规范

3 术语和定义

GB/T 36298—2018、GB/T 36319—2018、GB/T 36320—2018、GB/T 33190—2016 界定的以及下列术语和定义适用于本文件。

3.1

机构电子签约 institutional e-signing

机构之间的线上签约协作。

3.2

证书颁发机构 certificate authority

颁发数字证书的机构。

3.3

核验身份 check identity

核实验证用户身份。

示例：校验注册的数字身份信息，用户实名制信息等。

3.4

版式 fixed layout

将文字、图形、图像等多种数字内容对象按照一定规则进行版面固化呈现的一种格式。

[来源：GB/T 33190—2016，定义3.1]

3.5

版式文档 fixed layout document

独立于软件、硬件、操作系统、输出设备的版式文档格式。

[来源：GB/T 33190—2016，定义3.2]

3.6

版式文件 fixed layout file

版式文档不同表现形式，如代码形式、文档形式、表格形式等。

4 略缩语

CA：证书授权（certificate authority）

5 概述

机构电子签约平台（以下简称“签约平台”）为机构与机构之间提供基于区块链的线上化电子签约方案，签约平台联合纠纷处理机构、授时中心、CA机构、存证机构，通过区块链技术，保证机构在签约平台上合同的完整性、真实性、合法性。签约平台提供安全可信的签约环境，通过数字加密、数字摘要、隐私保护等技术保证签约机构的数据隐私和安全。签约平台提供高效的合同签署服务，通过权限隔离、区块链存证、跨链访问等技术提升合同签署、查询、验证服务的效率。

6 系统架构

机构电子签约业务为机构之间提供基于区块链的线上签约服务，一般包括签约发起方、签约参与方、签约平台、纠纷处理机构、授时中心、存证机构、CA机构等。机构电子签约业务相关方及交互如图1所示：

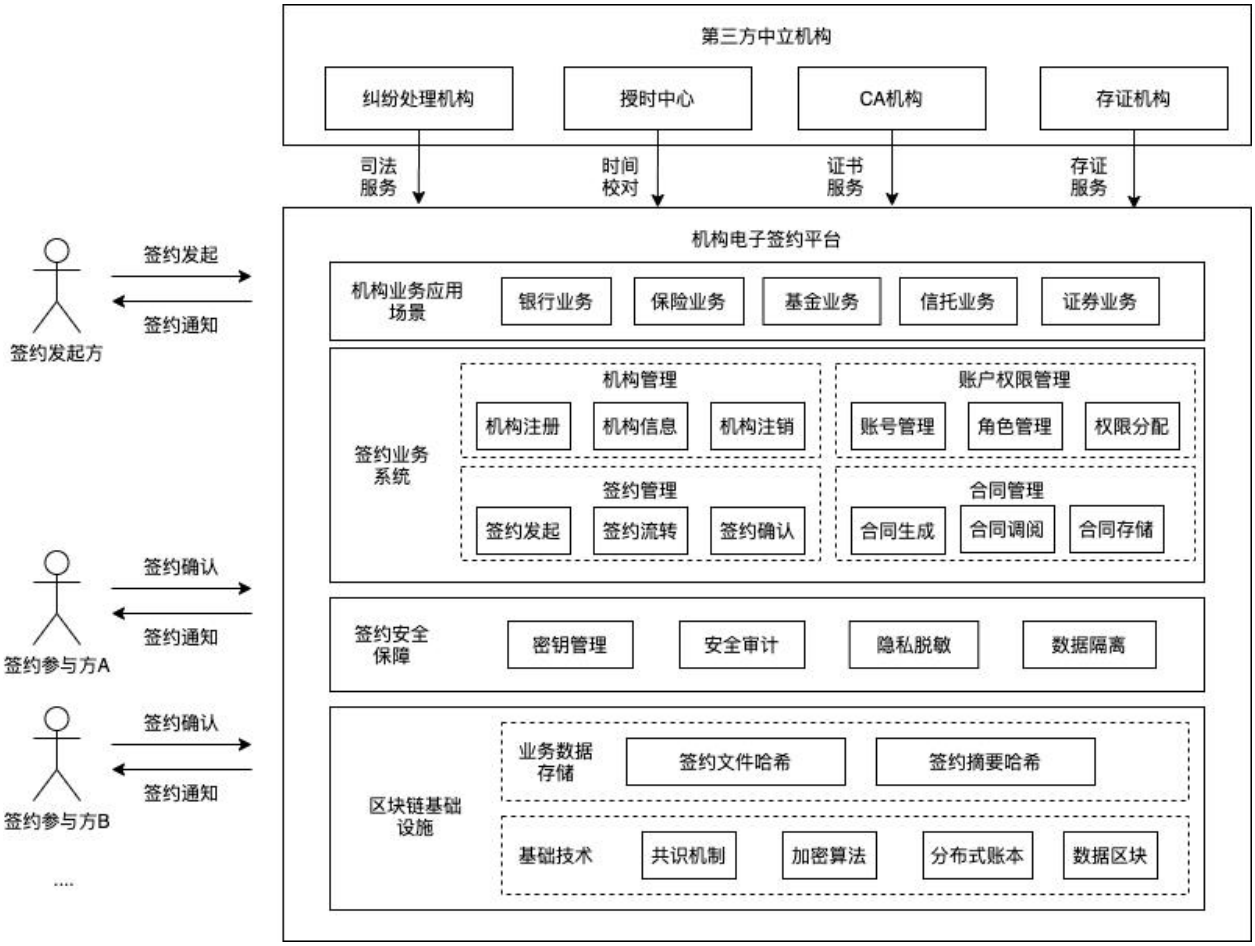

图 1 基于区块链的机构电子签约系统架构

6.1 签约主体

签约主体主要包括签约发起方和签约参与方：

a) 签约发起方：签约发起方可以发起一份合同的签约流程，指定各个签约参与方参与到签约流程中，包括但不限于银行、保险公司、基金公司、信托公司等相关机构；

b) 签约参与方：签约参与方在收到签约发起方的签约通知后，登录到签约平台上参与合同的签署，包括但不限于银行、保险公司、基金公司、信托公司等相关机构。

6.2 第三方中立机构

第三方中立机构不直接参与签约流程，在签约前、签约中、签约后的不同阶段中分别提供司法、时间、证书、存证等服务，通过区块链分布式存储、数字加密、数字摘要、数字证书等技术，保证签约的有效性、合法性。

a) 授时中心：国家授时中心，是我国唯一、专门、全面从事时间频率基础研究和应用研究的科研机构，为签约平台提供时间校准服务；

b) CA机构：负责发放和管理数字证书的权威机构，并作为电子商务交易中受信任的第三方，承担公钥体系中公钥的合法性检验的责任。可以通过CA机构在签约过程中为签约发起方和签约参与方颁发数字证书；

c) 存证机构：存证机构是第三方独立机构，接入机构电子签约区块链平台，通过见证、获取区块链上的存证信息；

d) 纠纷处理机构：法院、仲裁机构、公证处、司法鉴定中心等机构，当签约各方存在纠纷时，提供维权服务。

6.3 机构电子签约平台

机构电子签约平台为签约参与方提供可信电子签约服务，并且与第三方司法机构、CA机构、存证机构等进行密切合作。通过底层区块链平台，实现签约平台与司法机构、CA机构、存证机构之间的分布式数据共享，共同实现从签约流程到签约结果的线上可信签约业务。

a) 业务适用场景：签约平台适用于机构之间的可信签约，包括但不限于银行业务、保险业务、基金业务、信托业务、证券业务等。

b) 签约业务系统：系统包含机构管理、账户权限管理、签约管理、合同管理等模块。

1) 机构管理模块：负责机构的注册、机构信息存管、机构注销等功能；

2) 账户权限管理：负责机构的账号管理、账号角色管理、账号权限管理等；

3) 签约管理：管控整个签约流程，包括签约发起、签约流转、签约确认、签约通知等；

4) 合同管理：管理合同生命周期，包括合同生成、合同存储、合同调阅等。

c) 签约安全保障：签约平台提供完整的安全保障机制，包括但不限于用户密钥管理、用户操作安全审计、合同数据隐私脱敏、不同机构合同数据隔离等；

d) 区块链基础设施：区块链平台作为分布式数据存储平台，由签约平台与第三方中立机构联合运营，组成签约联盟链，签约平台在区块链上存储签约数据，包括签约文件的哈希值、签约摘要的哈希值，第三方机构通过比对原始数据与哈希值，可保证签约数据的真实性、完整性、不可篡改性。区块链基础技术由共识机制、加密算法、分布式账本、数据区块等组成。

7 业务流程

签约业务总体包含机构注册、机构签约、签约驳回、合同归档、签约存证、签约查询、机构注销等步骤，相关流程如图2所示：

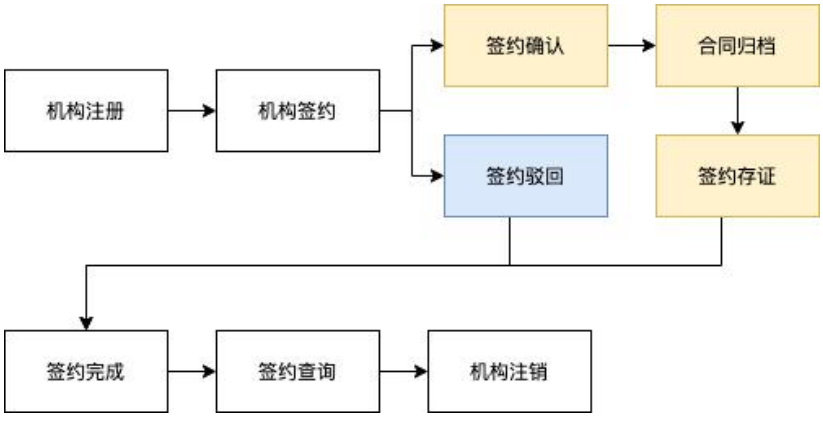

图 2 签约业务流程

7.1 机构注册

机构初次使用平台签约服务，应通过签约平台的账号注册流程进行机构注册。

具体业务流程如图3所示：

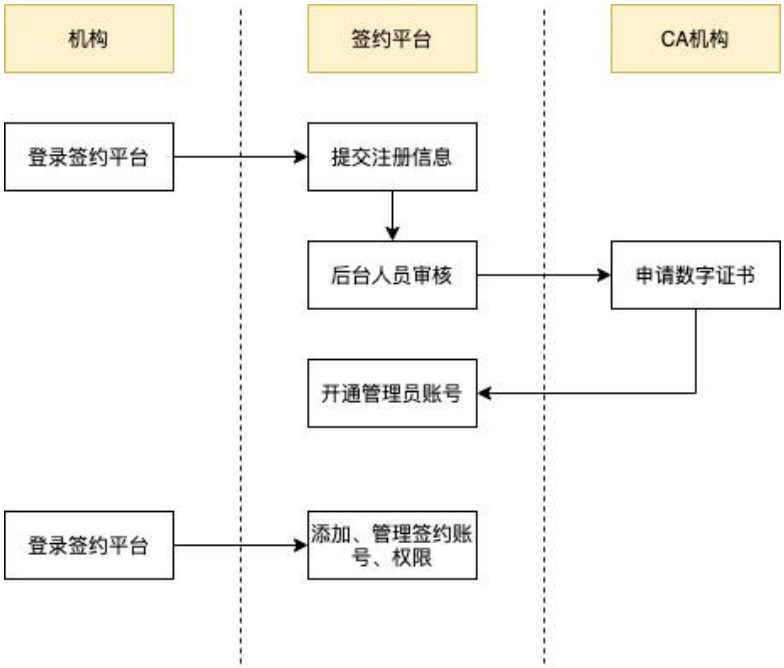

图 3 机构注册流程

a) 用户在首次登录时，应在签约平台上进行账号注册，在注册时应指定机构后续用于登录的管理员账号，同时该账号也作为机构身份的唯一标识；
b) 机构在注册时应提供必要的机构相关信息，包括但不限于机构名称、机构统一社会信用代码、机构营业执照副本、参与人具体信息（手机号码、身份证号、IP地址、MAC地址等）等；
c) 提交注册信息后，由签约平台的后台运营人员对注册信息进行审核，确保信息的真实性和准确性；
d) 审核人员通过审核后，签约平台自动为机构向CA机构申请机构数字证书，同时生成签约账号，并使用机构申请注册提交的账号作为机构在签约平台的管理员账号；
e) 机构开通管理员账号后，可以用管理员账号登录签约平台，并可在签约平台上添加新的机构内部员工账号，提供给内部员工（非管理员）登录签约平台，并根据公司内部治理制度给员工在签约平台上设定不同的权限。

7.2 机构签约

机构签约指签约发起方、签约参与方在签约平台上完成签约过程。相关业务流程如图 4 所示：

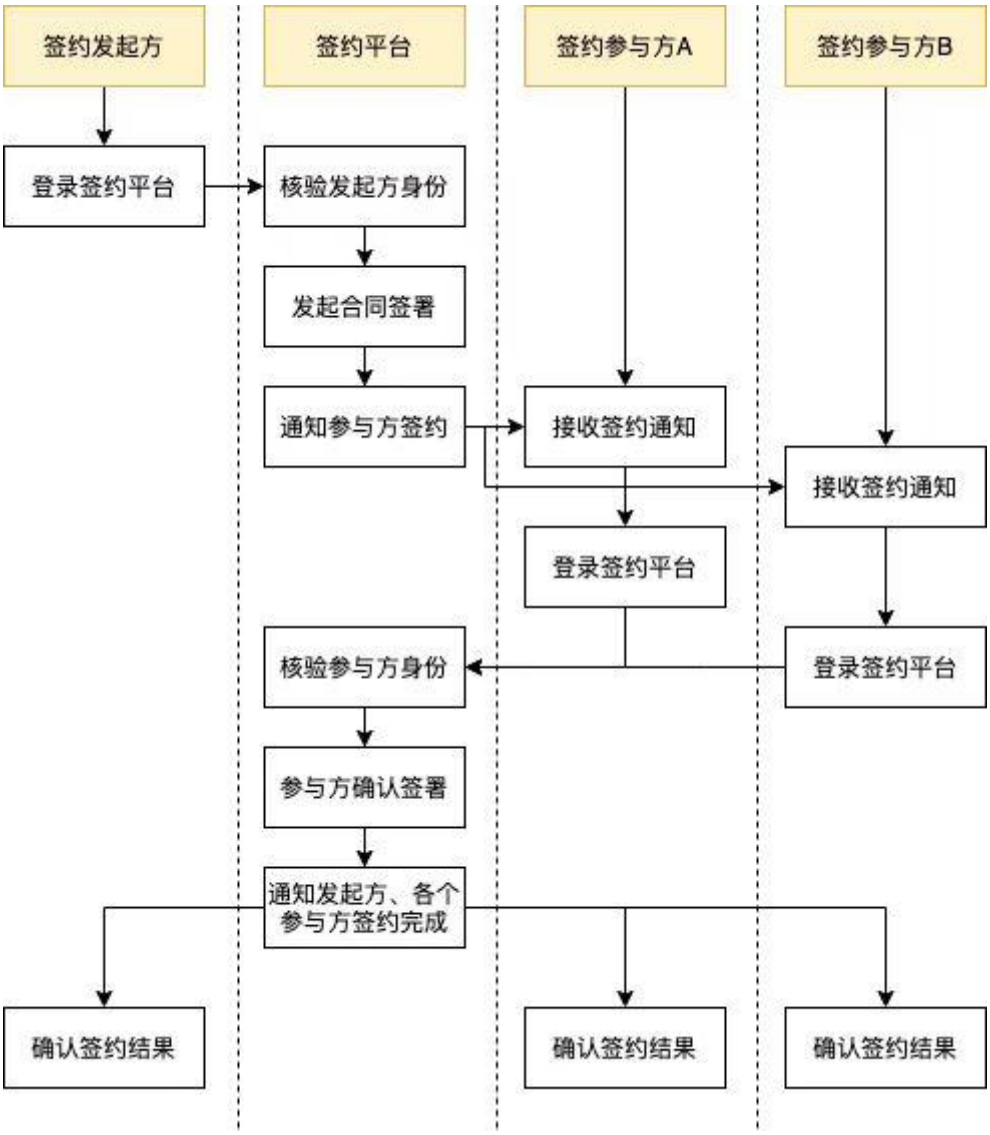

图 4 机构签约流程

a) 发起方登录签约平台，签约发起方可以通过其在签约平台的账号登录签约平台；

b) 核验发起方身份，签约平台对签约登录账号的权限进行校验，仅管理员账号或者是有签约发起权限的普通账号可以在签约平台上发起签约。核验权限通过后，签约平台还应通过密码、银行卡、人脸等核身方式核验签约发起方身份，确认签约发起方为登录人本人；

c) 发起方发起合同签署，发起方通过身份、权限验证后，在签约平台上上传合同文件副本，并制定合同签约的各个参与方，发起签约流程；

d) 通知参与方签约，签约流程发起后，签约平台通过邮件、短信、站内信等方式通知签约参与方，提醒参与方登录平台签约；

e) 参与方登录签约平台，签约参与方收到通知后登录签约平台，可通过邮件通知中的链接或签约平台网站登录；

f) 核验参与方身份，签约平台对签约登录账号的权限进行校验，仅管理员账号或者是有签约确认权限的普通账号可以在签约平台上确认签约。核验权限通过后，签约平台还应通过密码、银行卡、人脸等核身方式核验签约参与方身份，确认签约参与方为登录人本人；

g) 以下为参与方确认流程：

——参与方确认签署，参与方通过身份、权限验证后，在签约平台上可看到发起方发送过来的签约合同，阅读合同确认无误后，可在线点击确认签约；

——当所有参与方确认签署完成后，签约平台确认当前签约流程结束，并通过短信、邮件、站内信等方式通知签约发起方、各个签约参与方。

7.3 签约驳回

接收到签约发起方的签约后，参与方也可驳回发起方发起的签约，相关流程如图5所示：

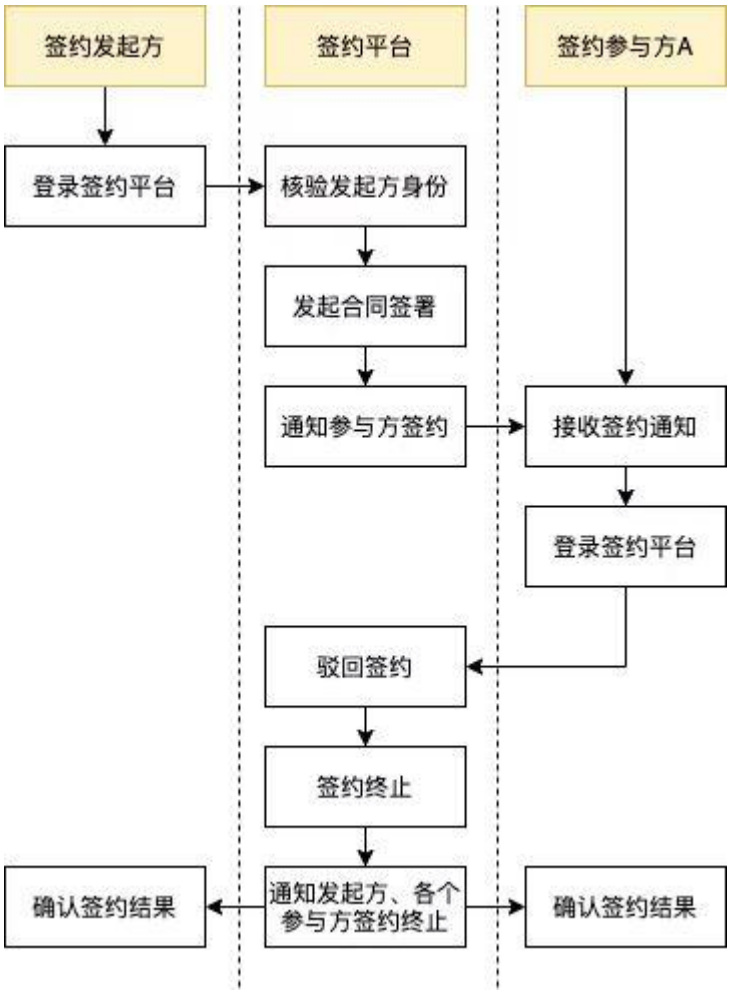

图 5 签约驳回流程

参与方驳回流程：

a) 参与方驳回，参与方通过身份、权限验证后，在签约平台上可看到发起方发送过来的签约合同，当对合同有异议时，可在线点击驳回签约；

b) 当任意参与方驳回后，签约平台确认当前签约流程终止，并通过短信、邮件、站内信等方式通知签约发起方、各个签约参与方。

7.4 合同归档

当各个参与方签署完毕后，签约平台自动对电子合同文件进行归档和存储，相关流程如图6所示：

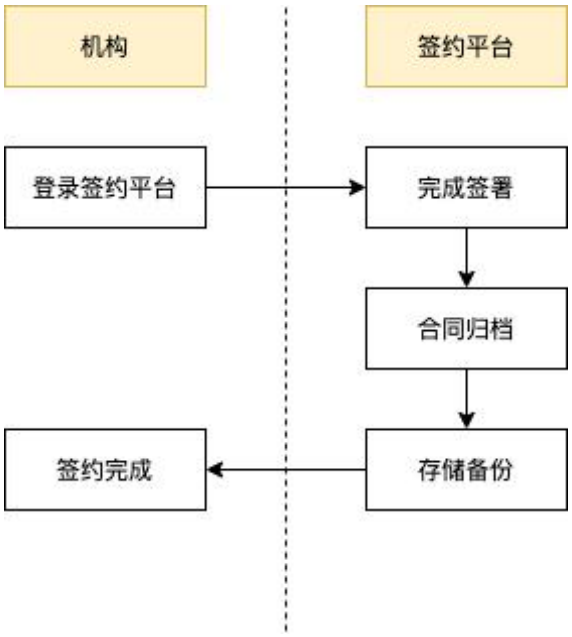

图 6 合同归档流程

a) 按照签约发起方、签约参与方分别对合同进行归档，保证发起方和所有参与方均能正确检索、查看合同；
b) 对合同中的关键信息，如发起方身份、参与方身份、签署时间等进行校验，确保合同的真实性、完整性和有效性；
c) 合同存储应支持数据备份，包括但不限于完整备份、条件备份、增量备份等方式。并能提供有效的存储状态监控，保障合同的存储安全。

7.5 签约存证

7.5.1 概述

签约存证是指签约平台将签约流程、签约结果，经过哈希运算之后，存储在区块链分布式存储上的行为，包括过程存证和结果存证两部分。相关流程如图7所示：

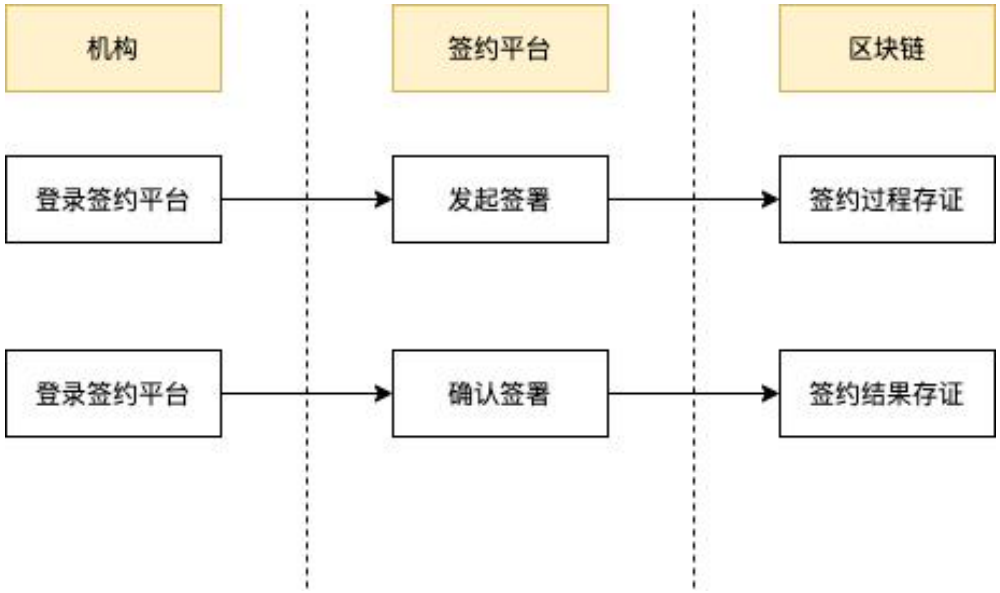

图 7 签约存证流程

7.5.2 过程存证

机构在签约平台的操作过程中，应将所有签约的流程信息作为日志摘要，对日志摘要进行哈希之后将哈希值存储到区块链平台存证，保证用户操作记录的完整性和不可篡改性。

其中涉及用户的相关操作包括但不限于如下数据：

a) 签约基本信息，应包括签约流水号、签约时间、签约当前所属阶段，其中不同阶段包括签约发起、签约确认、签约撤销、签约驳回等；

b) 当前签约方信息，应包括当前签约方的名称、证件类型、证件号、签约顺序、操作时间、核身时间、核身方式和核身结果；

c) 当前签约合同信息，应包括合同的名称、合同编号、合同版本、合同文件哈希值等信息。

7.5.3 结果存证

在签约流程结束以后，应将最终确认信息记录在链上，具体包括：

a) 合同最终确认信息，应包括合同名称、合同编号、合同版本、合同原始文件哈希值等信息，宜包括合同原始文件，视具体场景灵活选择；

b) 签约方信息，应包括不同签约方身份信息，如身份ID等；

c) 签约信息，应包括如签约时间、签名信息等。

7.6 签约查询

在签约完成后，机构可在签约平台上查询签约结果，包括签约时间、签约各个参与方、合同内容、区块链存证信息等。相关流程如图8所示：

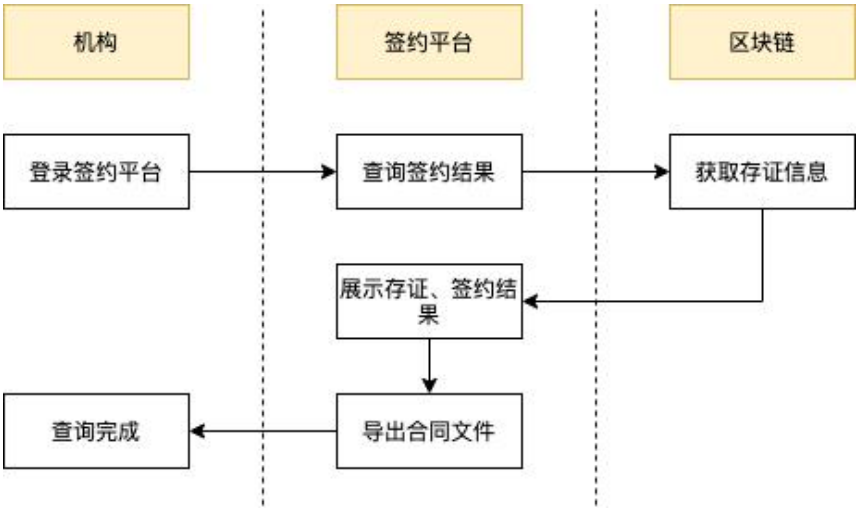

图 8 签约查询流程

a) 登录签约平台，机构可以通过其在签约平台的账号登录签约平台；
b) 查询签约结果，机构登录签约平台后，在线查询签约结果；
c) 获取存证信息，签约平台根据签约业务的唯一标识，从区块链上获取相关的存证信息；
d) 展示存证信息、签约结果，签约平台获取存证信息后，与本地数据库留存的签约基础信息一同展示给机构用户。

7.7 机构注销

当机构不再需要使用签约平台时，应在签约平台提交注销申请，注销后的机构历史签约信息仍保留在平台中，相关签约方可查询阅读。

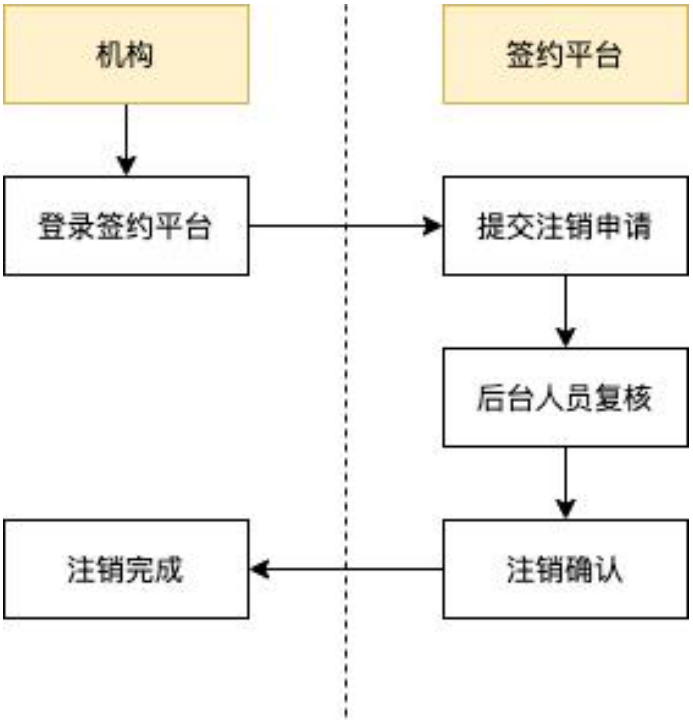

图 9 机构注销流程

a) 登录签约平台，机构在注销流程中应使用管理员账号登录签约平台；
b) 提交注销申请，机构管理员账号登录后，应在签约平台提交注销申请；
c) 后台人员复核，后台人员应复核机构申请，确认当前所有签约事项已完结，并与机构二次确认；
d) 确认注销，确认注销申请无误后，后台人员审核通过，确认注销；
e) 注销结果，账号注销后，签约平台中再无该用户，该用户无法再进行登录、新增、更新等操作，该用户注销前签署的历史合约等内容应得以保留，不受注销行为影响。

8 功能要求

8.1 业务功能要求

签约平台的业务功能以及相应性能要求如下：
a) 支持签约账户申请、开立功能，账户开立应在 3 秒内完成；
b) 支持机构账户管理、权限管理功能；
c) 支持机构线上签约发起签约功能，单次签约应在 5 秒内完成；
d) 支持多机构共同参与签约功能，单次签约应在 5 秒内完成；
e) 支持机构参与方确认签约、驳回签约功能，确认、驳回等操作应在 5 秒内完成；
f) 支持机构签约事件多渠道通知功能，且应保障通知时效，1分钟内触达用户；
g) 支持签约合同查阅、下载功能，单次查询应在 1 秒以内获得相关结果；
h) 支持签署过程、签署合同上链存证功能，上链过程应在 10 分钟内完成；
i) 支持签署过程、签署合同链上查询功能，合同单次查询应在 5 秒内完成；
j) 支持机构账户注销功能。

8.2 签约环境

签约环境要求如下：
a) 签约平台对每家机构的用户账户（包括管理员账户和普通账户）应严格管理，在用户登录时必须验证其账号密码的一致性；
b) 在签约服务的使用过程中，针对每个用户的登录状态，应按照要求设定其空闲时长，要求空闲时间不能超过30分钟，超过30分钟需要用户再次登录，以保证用户账户不被冒用；
c) 签约服务的代码编写必须安全可靠，代码编写完成后应进行代码安全审计；
d) 对签约平台应定期进行应用安全监测，防止应用出现SQL注入、XSS攻击、越权执行、目录遍历等安全漏洞；
e) 签约平台服务可用性应不低于99.99%，度量方法为（月可用时间/月总时间）*100%。

8.3 签约通知

签约通知要求如下：
a) 签约平台应具备多渠道通知能力，包括但不限于短信、邮件、站内信；
b) 应保障短信通知的时效性，在不超过1分钟之内触达用户；
c) 应确保邮件中到签约平台的跳转链接安全性，链接应设定有效期时长，不应长期有效，有效期不超过3个月；
d) 邮件中的链接不应包含明文信息；

e） 应保证链接不能由非签约平台伪造、推测；
f） 站内信应及时准确发送给签约各参与方，并以弹窗、消息数等方式进行提示。

8.4 数字证书

数字证书作为机构在签约中的身份标识，应具备如下特性：
——安全性，数字证书应保障使用者安全使用，密钥不能被他人伪造，数字证书仅由电子签名人控制；
——唯一性，针对不同用户不同证书，每一份证书应保证唯一性，不存在两份同样的证书；
——便利性，对于数字证书的使用应保证便捷，能即时申请、即时使用。

8.5 链上存证

链上存证要求如下：
a） 签约平台应对签约过程摘要和签约结果文件进行哈希计算，并通过区块链平台存储哈希数据，做为链上存证；
b） 存证数据所用哈希算法宜采用SM3国产哈希算法，哈希计算性能应不低于 5MB/s；
c） 存证数据应能与签约数据一一对应，通过存证哈希，能快速校验签约信息的准确性和有效性；
d） 存证数据应能高效在区块链中传播，第三方存证机构能通过区块链快速获取并记录存证结果。

8.6 跨链访问

考虑到区块链签约平台与其他系统的互操作性，签约平台宜通过跨链技术提供跨系统访问。
a） 签约存证应支持跨越不同的区块链系统执行；
b） 签约存证区块链中记录的存证数据，应能够被通过跨链技术接入签约区块链的系统访问和验证；
c） 跨链方案宜具备通用性、易用性，宜采用“非侵入式”方式和其他链系统交互，可兼容现有主流区块链系统；
d） 宜支持通过模板文件实现签约平台的跨系统互操作，相关可信交互包括：
——所述交易哈希附加在版式文件的数据单元上，允许接收者用以确认版式文件的来源和真实性；
——接收者解析版式文件的数据单元，以解析获取的交易哈希向发送者请求版式文件的数字摘要，校验前述数字摘要和签约文件数字摘要的一致性。

8.7 数据一致性

数据一致性要求如下：
a） 在区块链存储上，应通过链式数据结构、存储区块、标准时间戳等技术，实现签约存证的可靠、不可篡改、不可伪造等特性；
b） 签约平台应具备统一的数据处理规则，签约系统和区块链结合保证区块链结点上的数据在经过各节点广播、共识或同步后，数据在区块链的不同节点上的结果应保持一致；
c） 区块链上的不同节点，应采用适应性强的共识算法，保障签约数据在链上不同节点之间的同步效率；
d） 签约平台、区块链应采用国产密码算法 SM2、SM3、SM4、SM7、SM9 等进行摘要计算、数据加密，并通过加密技术确保信息安全防护等级，从而保障区块数据的一致性、有效性与可靠性。

8.8 共识机制

共识机制要求如下：

a) 各区块链节点能够快速达成共识，支持高效共识匹配网络扩容、高速签名等技术。
b) 在共识过程中，各网络节点要确保交易有序且交易区块有效，各结点共识应在 10 分钟内完成，且应具备以下核心功能：
——交易有效：根据交易验证及背书策略确保区块中所有交易有效；
——交易有序：确保所有节点提交和执行交易顺序的最终一致性；
——交易验证：利用智能合约的接口，验证交易的有效性和顺序一致性。

9 安全要求

9.1 账户安全

机构可在签约平台上注册多个账户，账户分为两类：管理员账户、普通账户：

——管理员账户：在签约平台上，一个机构由一个管理员进行账户管理，管理员账户由机构在签约平台注册时自行指定，指定后即与该机构身份进行绑定，由签约平台对认证信息审核，不能更改。管理员账户拥有最高权限，能够在签约平台进行任何操作；

——普通账户：管理员账户可自行添加通过本公司认证的普通账户，普通账户在签约平台进行相关的日常操作事宜，其操作权限通过管理员来分配。

账户安全要求如下：

a) 机构签约应明确区分包含但不限于如下权限：签约发起、合同查阅、签约确认、合同下载、存证查询等；
b) 管理员拥有对应机构在签约平台上的所有操作权限（如签约发起、合同审阅、合同下载、存证查询等）；
c) 普通账户的操作权限应由管理员进行分配，不同的普通账户权限隔离，获得权限的用户可在签约平台上进行对应权限的操作，未获得授权用户无法进行相关操作；
d) 签约平台应对每个用户有一个单独的标识，每个账户有单独的登录账号，登录账号密码必须为强口令密码，不应使用弱口令，密码复杂度应满足要求：
——包含大写字母、小写字母、数字；
——密码位数大于8位。
e) 对于管理员账户，签约平台应在机构注册时对其身份进行审核，确认无误后，生成管理员账户标识；
f) 普通账户应由机构管理员自行审核。

9.2 身份安全

要求如下：

a) 不应在未验证用户身份的情况下进行签约发起、签约确认、合约查询等相关操作，可浏览阅读如平台介绍、操作指引等与用户身份无关的公开信息。
b) 用户身份认证应通过人脸认证、密码认证两种方式进行，优先通过人脸识别，识别用户身份，如果人脸不通过，再通过密码识别。

9.3 环境安全

要求如下：

a) 签约平台的计算机硬件、附属通信设备及网络传输线路应稳定可靠，机房安全稳定。平台的前台系统、后台系统、数据库服务均应进行安全隔离。网络信息传输过程中不能被他人窃取、篡改，只有经过授权的用户才能使用和访问；
b) 签约平台应对系统设备的运行情况、网络流量、用户行为等进行监控和审计，针对运行中的异常具备完善的报警和应急能力；
c) 签约平台所使用操作系统应遵循最小安装原则，仅安装必要的应用程序，并对操作系统定期更新维护，及时安装系统安全补丁，关闭不必要的服务和端口。
d) 应对操作系统的访问权限进行严格区分，禁止使用默认账户和匿名账户，定期更换账户密码。

9.4 数据安全

9.4.1 数据加解密

要求如下：
a) 为保障签约合同的保密性，签约平台对关键合同数据应进行加密后存储，防止非授权用户截获使用；
b) 签约平台应妥善保管合同数据的加解密密钥，密钥应单独设置，不应与服务器登录、账号登录等密钥混用。

9.4.2 数据脱敏

经过数据脱敏处理后，已知的敏感信息已经被隐藏和处理，但脱敏后的数据由于保持了原始数据的部分统计特征和结构特征等信息，仍可能存在一定的敏感信息泄漏风险。数据脱敏要求如下：
a) 应采取合适的方式控制知悉范围，通过恰当的安全管理手段，防止数据外泄。
b) 在签约系统平台上，为了保障用户信息不被泄露，所有日志数据应做数据脱敏处理，脱敏字段包括但不限于客户名称、证件号、手机号、邮箱、固定电话、银行卡、通信地址等；

9.4.3 数据隔离

9.4.3.1 不同机构之间的数据隔离

在签约平台的数据设计中，应明确每家机构的身份标识，签约平台应按机构标识字段区分机构数据，当进行查询时根据机构身份标识区分机构合约数据，确保机构之间数据不能交叉访问。

9.4.3.2 后台访问数据访问控制

针对后台数据访问，应严格控制访问权限，根据不同的权限设置不同的数据隔离级别，至少设置三层权限：
a) 最高管理员：最高管理员可查阅、下载、与本公司签约的所有合同文件，文件中包含合同完整内容信息；
b) 业务管理员：业务管理员可查阅、下载与本业务部门相关的合同文件，文件中包含合同完整信息，不能跨业务访问；
c) 业务操作员：业务操作员仅可访问与本业务部门相关的，并且关键信息脱敏后的合同信息。不能查看、下载合同原文。

9.4.4 存储安全

签约平台的数据存储安全应包括电子文件存储安全、存储介质安全和灾备安全：

a) 电子文件存储安全：电子文件宜依据《中华人民共和国电子签名法》生成，且独立于软件、硬件、操作系统、输出设备的开放式版式文档，宜采用分布式文件系统或去中心化方式存储；
b) 存储介质安全：对承载数据的物理实体介质（磁盘、硬盘）或虚拟存储介质（容器、虚拟盘），应对介质访问和使用行为进行记录和审计；
c) 数据容灾安全：签约平台的数据可支持分布式存储框架，使用多个存储服务器共享存储负载，提高数据可靠性、可用性和访问效率，实现跨数据中心和跨地域的容灾，具备定期归档备份机制，提升系统容灾防护能力。

9.5 网络安全

不同参与方之间、系统不同部分之间的通信网络，要求如下：
a) 应具备安全防护机制，如身份认证、TLS 加密、敏感内容脱敏等；
b) 网络层面，宜具备常见网络攻击防护能力，如能够有效抵御 DDoS 攻击、女巫攻击、日蚀攻击等。

9.6 安全审计

要求如下：
a) 在用户登录到签约平台后，对用户的任何操作均应保留用户的操作记录，保证签约过程可审计、可回溯；
b) 用户在签约过程中应对合同文件完整全面的阅读，确保对合同的充分理解，签约平台应保存但不限于如下数据信息：
——平台登录信息：记录平台登录人身份信息、登录人所属机构、登录时间信息；
——合同阅读次数：记录登录人在确认合同之前阅读合同的次数；
——合同操作时间：记录登录人阅读合同完毕后，对合同的相关操作时间，操作应包括但不限于合同发起、合同确认、合同撤销、合同驳回等。

附 录 A

（资料性）

跨平台签约场景示例

A.1 场景描述

签约参与方甲、乙共同参与签约，其中，甲使用联盟链 A，乙使用联盟链 B，A 和 B 为不同的区块链系统。

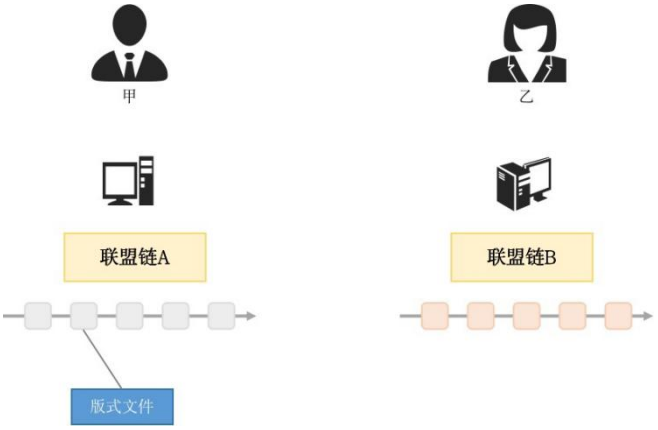

图 10 使用不同区块链系统的甲乙双方进行跨平台签约

A.2 跨平台签约流程

甲乙双方进行跨平台签约流程如下图所示：

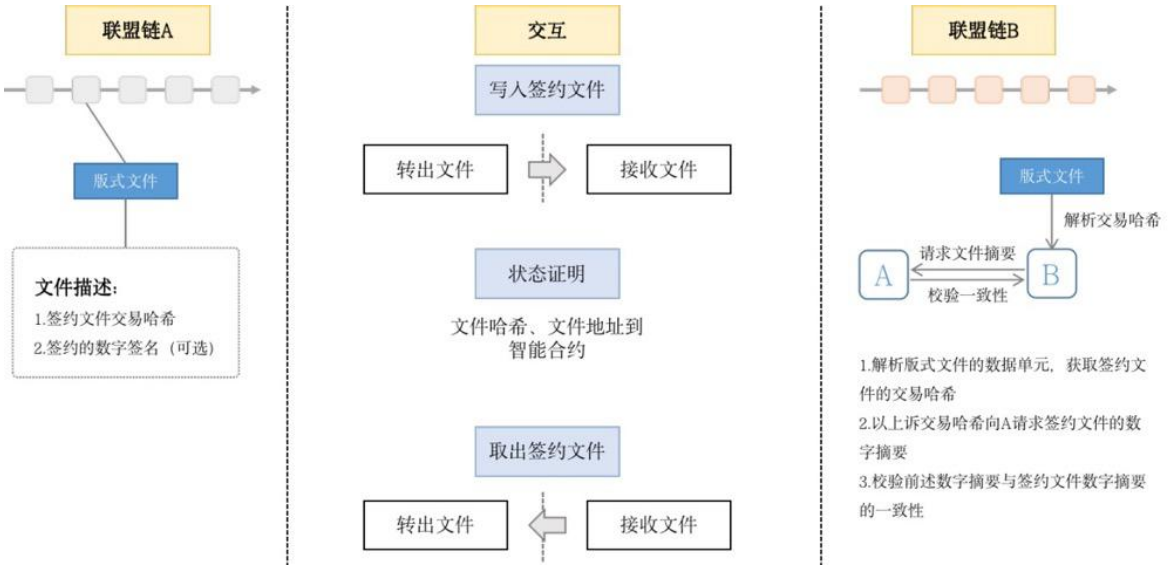

图 11 甲乙双方跨平台签约流程示意图

a） 联盟链 A 在所述版式文件中写入签约文件的交易哈希；

b) 联盟链 B 通过交互获取前述版式文件，解析文件中的交易哈希；
c) 联盟链 B 通过前述解析的交易哈希向联盟链 A 请求对应文件的数字摘要；
d) 联盟链 B 校验文件的数字摘要是否一致；
e) 联盟链 B 完成会签操作。