云链金融平台
安全解决方案

中金金融认证中心有限公司

2015 年 7 月

目录

1 引言

1.1 文档目的

本文档是中金金融认证中心（以下简称 CFCA）为中企云链编写的供应链融资平台安全解决方案。

1.2 读者对象

相关方业务管理人员、系统建设人员及其他需要了解方案的人员。

1.3 参考文献

《中华人民共和国电子签名法》
《公钥基础设施 PKI 与认证机构 CA》

1.4 基本术语

RA：证书审核注册中心 - Registration Authority，是 PKI 体系中的注册审批系统，它是 CA 的组成部分和面向用户的延伸。

电子签章：是电子签名一种表现形式，利用图像处理技术将电子签名操作转化为与纸质文件盖章操作相同的可视效果，同时利用电子签名技术保障电子信息的真实性和完整性以及签名人的不可否认性。

证书工具包：用于实现数字证书各项功能的中间件产品，支持数字签名和验证功能，支持浏览器调用以及服务器端的 Java 调用。

借款方：平台上申请贷款的一方，通常要对其进行严格的身份审核和资产状况评估，因此借款方一般都会采用线下面签的形式开通、注册用户。

2 建设背景

2.1 现状概述

随着社会化生产方式的不断深入，市场竞争已经从单一客户之间的竞争转变为供应链与

供应链之间的竞争，同一供应链内部各方相互依存，“一荣俱荣、一损俱损”；与此同时，由于赊销已成为交易的主流方式，处于供应链中上游的供应商，很难通过"传统"的信贷方式获得银行的资金支持，而资金短缺又会直接导致后续环节的停滞，甚至出现"断链"。维护所在供应链的生存，提高供应链资金运作的效率，降低供应链整体的管理成本，已经成为各方积极探索的一个重要课题，因此“供应链融资”系列金融产品应运而生。

2011 年以来，各家商业银行受到信贷规模的限制，可以发放的贷款额度十分有限，但是通过承兑，票据、信用证等延期支付工具，既能够增强企业之间的互相信任，也稳定了一批客户，银行界空前重视供应链金融业务。目前，商业银行在进行经营战略转型过程中，已纷纷将供应链金融作为转型的着力点和突破口之一。供应链管理已成为企业的生存支柱与利润源泉，几乎所有的企业管理者都认识到供应链管理对于企业战略举足轻重的作用。

面对国内互联网金融的飞速发展，传统线下的供应链金融模式已经很难满足企业客户对于高效、便捷、不受时空限制的需求，利用线上供应链金融平台实现线上业务办理已是趋势。由于传统供应链金融采用现场面对面确认和成熟的业务操作流程，采用互联网模式的供应链金融平台面临的最大的挑战还是风险管理，包括规避法律风险、交易风险、技术风险等，为解决以上业务安全问题，在整个业务通过引入 CFCA 数字证书体系，一方面成熟的电子签名、加密技术解决了平台的交易风险和技术风险，另一方面符合签名法相关规定的电子签名有效的规避了平台的法律风险。

2.2 需求分析

2.2.1 业务概述说明

1、预付款类融资场景：

融资企业向金融机构申请预付款融资，使用融资企业和核心企业签订的购销合同（即订单）及缴纳一定比例的保证金，同时未来该笔货物给金融机构办理质押，通常包含先票后货、未来货权质押融资等。

2、存货类融资场景：

融资企业以其合法持有且金融机构认可的动产/货权凭证（包括：仓单、提单）作为质押担保物，向金融机构申请贷款，通常包含动产质押、存货质押、标准或非标准仓单质押等。

3、应收账款类融资场景：

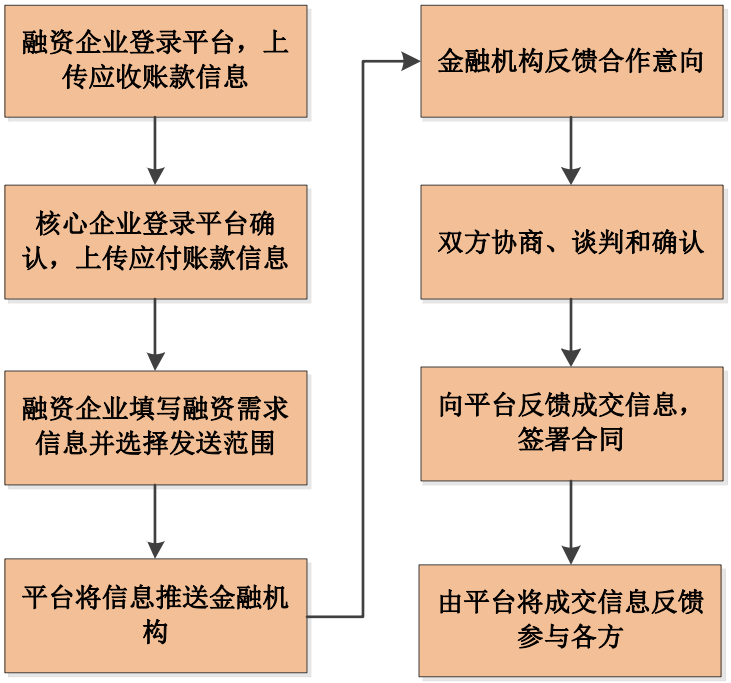
融资企业将供应链上核心企业未到期的应收账款单据凭证作为质押担保物，向金融机构

办理融资的行为，主要有应收账款质押、国内保理等。

整个供应链金融平台主要包含的参与方有：金融机构（资金提供方）、供应链金融平台（平台提供方）、融资企业（资金需求方）、核心企业（融资企业交易对手方）。

2.2.2 关键业务

供应链金融平台的关键业务为融资需求成交，具体如下（以应收账款场景为例）：



图标 2-1：关键业务流程

1、融资企业（应收账款债权人）登录供应链金融平台（以下简称平台），上传应收账款信息，由平台方推送在平台注册的相应核心企业（应收账款债务人）对其真实性进行确认；

2、核心企业向平台上传应付账款信息，该操作为对账款信息真实性的确认；

3、融资企业在平台确认应收账款的真实性之后，填写融资需求并选择发送范围；

4、融资需求通过平台推送至在平台注册的金融机构（资金提供方）；

5、金融机构通过平台对该笔有效需求的融资意向信息反馈给融资企业；

6、金融机构和融资企业双方协商、谈判，达成融资交易的确认；

7、金融机构和融资企业在平台填写应收账款融资成交单，包含应收账款债权转让/质押信息，在线签署合同（即成交单）；

8、由平台将该合同信息发送至融资企业、核心企业和金融机构。

2.2.3 关键需求

根据供应链金融平台业务的特点，在平台中需要解决以下三个主要问题：如何保障平台用户的身份真实可靠？如何保障平台签署的电子合同具有法律效力？如何保障用户操作信息和文件的不可抵赖、防篡改和保密？需求主要体现以下几点：

- **保障平台用户身份的真实性**

线下面对面并使用纸质证件代表参与各方的身份，线上使用数字证书实现高强度的身份验证解决用户身份真实性的问题。

- **保证平台上签署的电子合同具有法律效力**

在平台签署电子合同时使用电子签名技术，符合电子签名法的要求，从而保证平台签署的电子合同具有法律效力。

- **对用户信息做到防篡改和保密**

平台各参与方的关键交易（如签署电子合同）包含敏感业务信息，使用签名和加密技术实现敏感业务信息的防篡改和保密。

- **平台对用户的易操作性**

数字证书和签名技术已经是广泛应用的成熟技术，目前在网上银行广泛使用，平台用户已经成熟掌握该技术的操作和使用。

3 方案总体设计

3.1 设计原则

交易市场数字证书及数字签名安全系统的总体设计和实施，将依据国家有关信息安全政策、法规，根据中企云链实际需求，结合业内最佳实践进行设计。

- **先进性**

采用的技术与设备应具有先进性，符合当前技术和管理发展的方向，并确保该技术和设备有应用先例，且成熟、可靠、稳定。

- **稳定性**

系统应具备长期、稳定运行的能力，并具有良好的容错性能，在一定程度的事件或灾难

发生时，仍能保证 RA 系统不间断运行。

- **安全性**

系统建设应采用全面的安全防范技术和措施，保障平台信息和数据安全，保障网站的长期、稳定、可靠运行。

- **标准化**

采用符合国际、国家标准的软件，遵循有关技术规范体制，使系统具有灵活的互联能力。

- **扩展性**

RA 设计应充分考虑未来业务和技术发展的需要，具有功能扩展的灵活性和跨平台的可移植性，能快速、平稳地实现应用规模的扩展和技术升级。

- **开放性**

RA 系统设计在网络通信、数据交互等方面应遵循业界流行的开放标准，支持各种常用标准接口和协议。

- **合规性**

保证操作行为的真实、可靠且具有法律效力，符合《中国人民共和国电子签名法》的要求；保证操作流程及数据安全符合相关法律法规的要求。

3.2 建设目标

- **建设简单、可信的身份认证机制**

为平台参与方颁发企业用户证书，实现在登录和业务操作时对用户身份的认证；

为平台应用服务器颁发服务器证书，实现在对平台应用系统的身份认证。

- **建设安全的数据安全传输机制**

为平台配置 SSL 安全通道，使平台方与其他各方交互的数据加密传输。

- **建设权威、具有法律效力的防篡改机制**

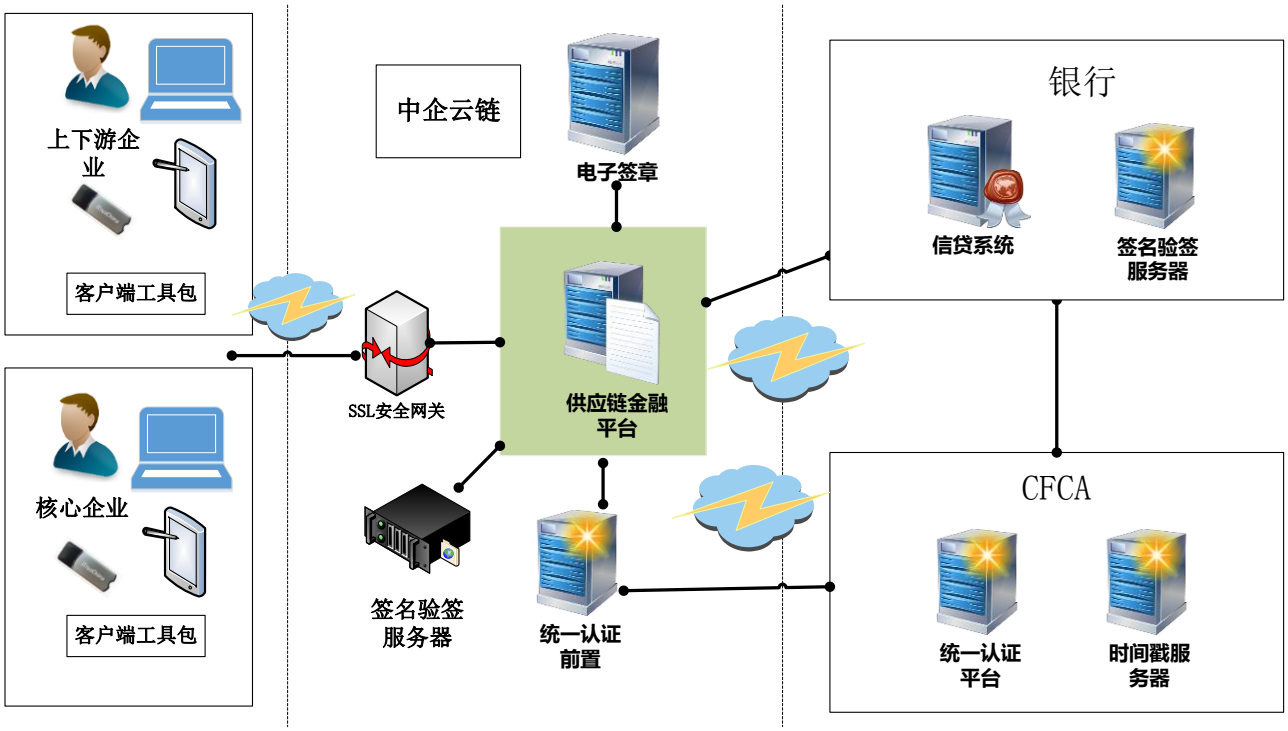
用户在登录或操作核心业务时，使用数字证书对业务动作进行签名，符合我国相关法律要求，使用户线上的交易行为具备法律效力。

- **建设易用的业务操作平台**

优化业务操作平台，在使用证书和签名技术的同时，提供良好的展示和操作机制使用用户操作安全的同时做到平台的易操作。

3.3 总体架构

CFCA 是自《电子签名法》颁布后，首批拿到《电子认证服务许可证》资质的第三方 CA 公司之一，其所发放的数字证书所做电子签名，完全符合《电子签名法》。同时 CFCA 结合在金融行业及其他行业中的经验和教训，从法律政策、技术需求等几个方面为中企云链设计的数字证书安全方案如下：



图表 3-1：中企云链证书应用总体方案

以 PKI/CA 技术为基础，通过国家授权的第三方电子认证机构——CFCA 为中企云链供应链金融平台用户发放企业数字证书实现整体应用的安全，具体如下：

1. 在中企云链平台客户端中集成证书工具包，包含 PC 端和 PAD 端，可在登录、电子协议签署等环节实现强身份认证、资金安全、电子协议合法合规性；
2. 在中企云链平台中服务器端集成签名验签服务器，可在登录、电子协议签署等环节实现强身份认证、资金安全、电子协议合法合规性；
3. 在中企云链平台中集成电子签章组件，实现电子协议电子签名可视化，提高用户体验，在签署协议时，各方可采用各自的数字证书和电子签章对协议进行签署，在保障合同协议合法合规性的同时，实现了电子协议可视化电子签章；
4. 可为中企云链平台发放全球服务器证书，对中企云链平台进行实名认证，通过对网站域名信息、主体身份信息、域名权属信息等进行严格审核，并利用 PKI 数字签名技术

形成不可篡改的认证标识，在浏览器上以安全可靠的方式进行展示，使中企云链平台用户更直观判断网站的真实身份防止钓鱼网站，同时可建立加密通道；

5. 在中企云链部署统一认证前置，已经拥有 CFCA 网银证书的企业可以将证书信息和企业身份信息通过统一认证前置向 CFCA 统一认证平台发起身份鉴权请求完成实名认证；
6. 在中企云链平台客户端中集成密码安全控件，实现对登录密码等私密信息的防护和加密，防止不法分子窃取关键私密信息；
7. 在中企云链平台前端搭建 SSL 安全网关设备，部署服务站点证书，实现用户访问网站时建立安全加密通道；
8. 在中企云链平台集成时间戳应用，使得所有电子协议/电子借据等电子文档在签署时间上同样具有可靠时间法律依据；
9. 所有签署的证书密文、电子签名、签署者公钥等；有效的保证了出现协议纠纷后，公证的还原相关协议原文和电子签名值。
10. 当发生纠纷时，CFCA 后期可为用户提供电子取证服务，可出具第三方取证报告。

3.4 方案产品

序号	产品名称	功能	说明	备注
1	PC 端证书工具包	PC 端实现客户端签名验签、加解密	部署在 PC 端	必须
2	签名验签服务器	硬件服务，实现服务端签名验签、加解密	部署在后台应用	必须
3	电子印章	实现对电子文档的签章、验章	部署在后台应用	必须
4	统一认证前置机	用于对用户和证书的有效性进行校验	部署在后台应用	必须
5	PC 端密码安全控件	PC 端保护用户输入密码敏感信息安全	部署在 PC 端	建议
	移动端密码安全控件	移动端保护用户输入密码敏感信息安全	部署在移动端	建议
6	SSL 安全网关	身份验证和建立 SSL 安全	部署在应用平台前端	建议

		通道		
7	时间戳服务	时间戳申请和验证	在线访问服务	建议

图表 3-2：方案产品

4 建设方案详细介绍

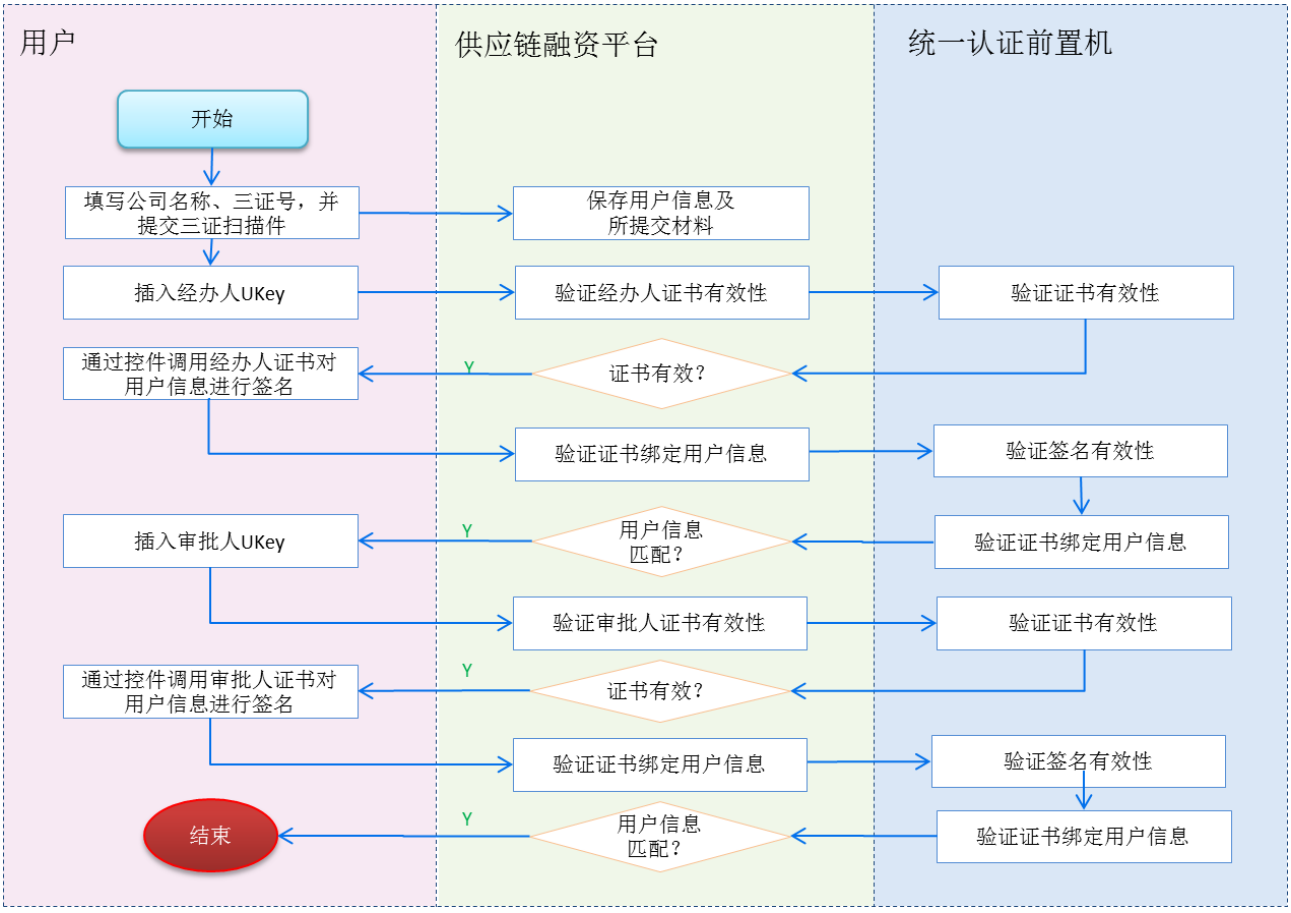
CFCA 提供的数字证书解决方案，从实名认证、关键交易签名、电子合同安全应用等几个角度，有效的解决用户身份真实性、所签署电子协议的法律有效性问题，保障供应链融资平台数据传输的真实性和机密性，同时能防止钓鱼攻击。以下针对不同业务场景进行业务流程设计。

4.1 实名认证-UKey 验证及绑定

4.1.1 场景说明

企业用户注册并登录系统后可进行实名认证。实名认证过程中要求用户填写公司全称，上传相关营业执照号、税务登记证号、组织机构代码号及三者扫描件。完成后验证和绑定用户的两个 UKey，验证目的：确认上述已填的企业信息与 UKey 的登记企业是否一致，要求能返回给平台 UKey 登记企业的全称。UKey 绑定：将用户手中的两个 UKey 分别与经办权限和审批权限绑定，此过程要求返回 UKey 的 DN 号。

4.1.2 业务流程设计



如上图所示，具体流程如下：

1、用户根据系统提示，填写公司全称、营业执照号、税务登记证号、组织机构代码号并提交三证复印件；

2、供应链融资平台保存用户提交的信息及材料，并提示用户插入支持的银行 UKey；

3、用户根据系统提示插入经办人 UKey，并选择经办人证书，通过控件获取**证书序列号**、**DN** 和**颁发者**，提交给供应链融资平台，平台通过调用统一认证前置机接口验证该证书是否有效（处于激活状态，未过期且未吊销）；

4、验证经办人证书有效性通过后，用户端浏览器通过调用签名控件，使用经办人证书对用户信息进行签名，提交到供应链融资平台；

5、供应链融资平台通过调用统一认证前置机接口，验证签名有效性，验证提交的用户信息是否匹配，如果不匹配，供应链融资平台可通过前置机接口查询该证书注册时的公司全称；

6、验证经办人 UKey 的用户信息通过后，用户根据系统提示插入审批人 UKey，并选择审批人证书，通过控件获取**证书序列号**、**DN** 和**颁发者**，提交给供应链融资平台，平台通过调用统一认证前置机接口验证该证书是否有效（处于激活状态，未过期且未吊销）；

7、验证审批人证书有效性通过后，用户端浏览器通过调用签名控件，使用审批人证书对

用户信息进行签名，提交到供应链融资平台；

8、供应链融资平台通过调用统一认证前置机接口，验证签名有效性，验证提交的用户信息是否匹配，如果不匹配，供应链融资平台可通过前置机接口查询该证书注册时的公司全称；

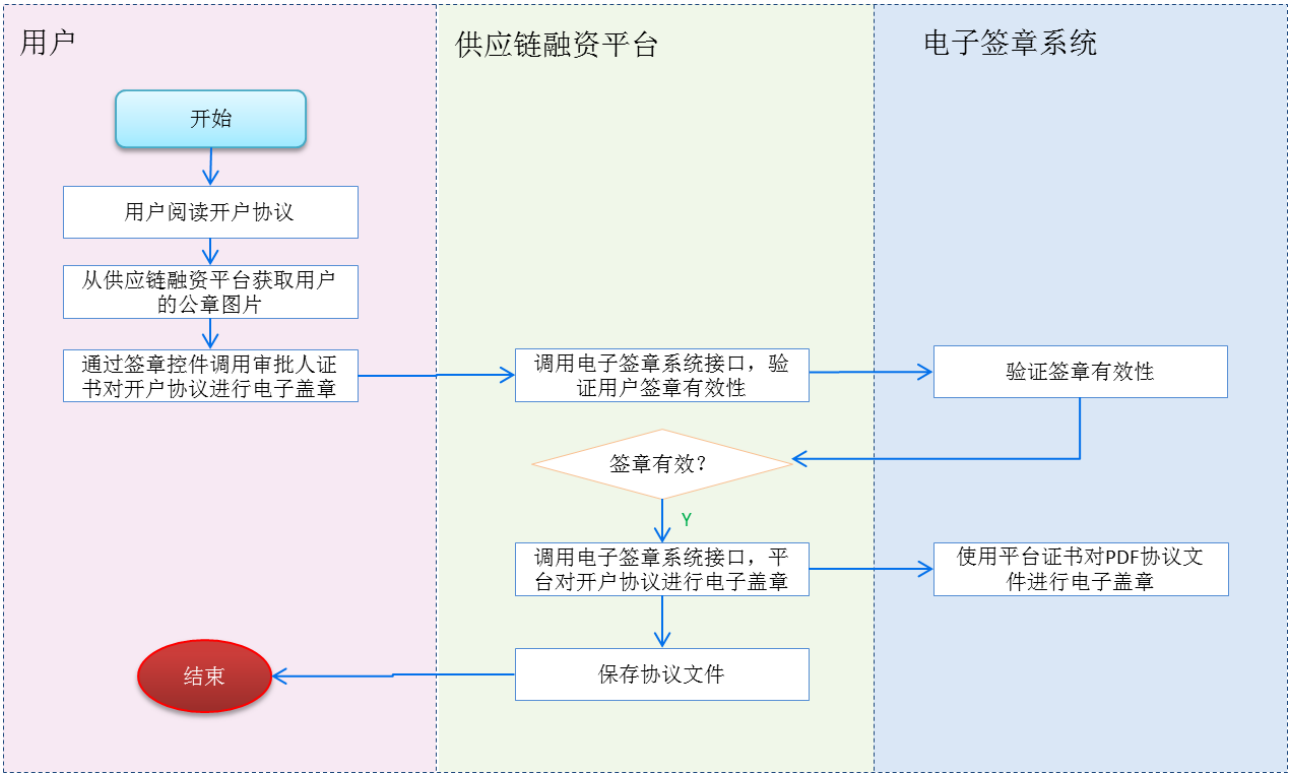
9、验证审批人 UKey 的用户信息通过后，实名认证过程成功完成。

4.2 开户

4.2.1 场景说明

开户过程用户需要签订开户协议，只需要一级 UKey 确认按钮（审核 UKey），验证 UKey 身份后通过 UKey 对协议（PDF 格式）加盖公章。

4.2.2 业务流程



如上图所示，具体流程如下：

1、用户阅读开户协议；

2、同意开户协议内如后，点击“同意”按钮，从供应链融资平台获取该企业的公章图片；

3、插入审批人 UKey，通过签章控件调用审批人证书对开户协议进行电子盖章，并提交给供应链融资平台；

4、平台调用电子签章系统接口，验证签章有效性；

5、如签章有效，则平台调用电子签章系统接口，对协议文件进行盖章；

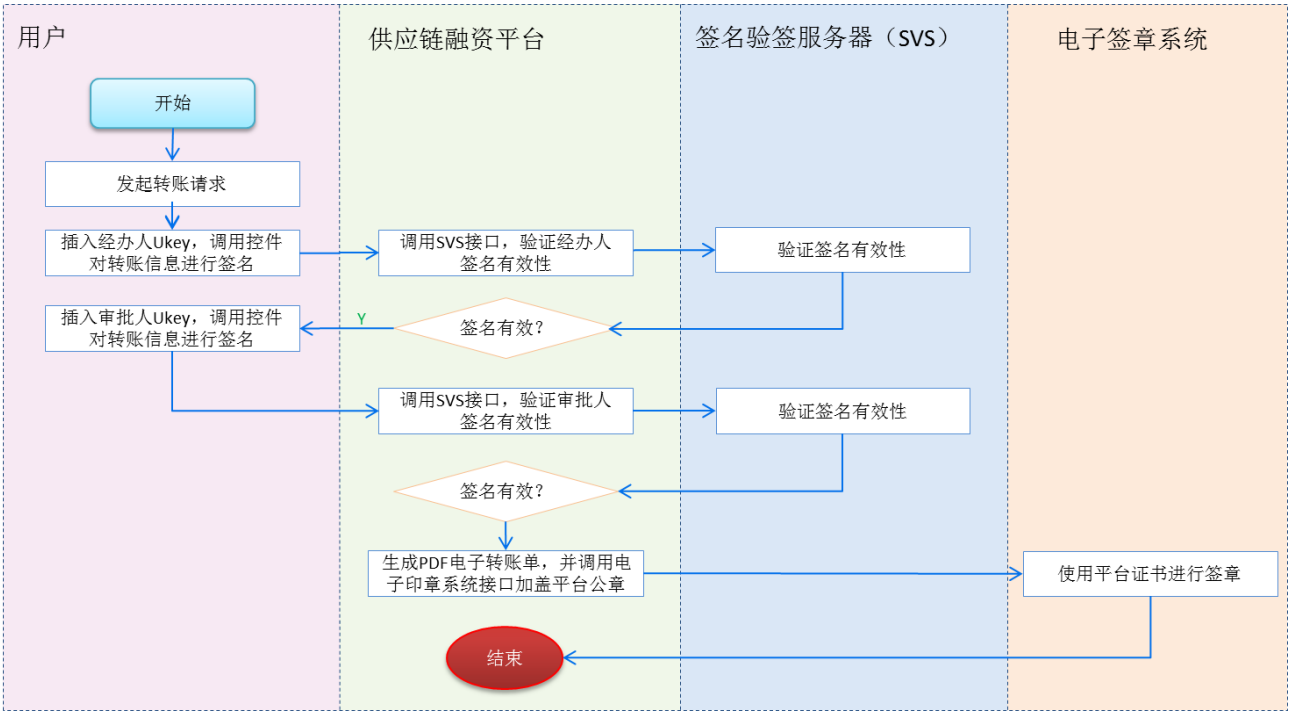
6、平台保存经双方盖章的协议，开户成功完成。

4.3 转账

4.3.1 场景说明

通过平台账户向其他账户转账，此过程需要两级 UKey（经办、审核）确认，验证身份通过后，在电子转账单上加盖公章。

4.3.2 业务流程



如上图所示，具体流程如下：

1、用户发起转账请求；

2、提示用户插入经办人 UKey，并调用控件对转账信息进行签名，提交给平台；

3、平台调用 SVS 接口，验证经办人的签名是否有效；

4、如果签名有效，则提示用户插入审批人 UKey，并调用控件对转账信息进行签名，提交给平台；

5、平台调用 SVS 接口，验证审批人的签名是否有效；

6、如果签名有效，则生成 PDF 格式的电子转账单，并调用电子签章系统，对电子转账单加盖平台的公章；

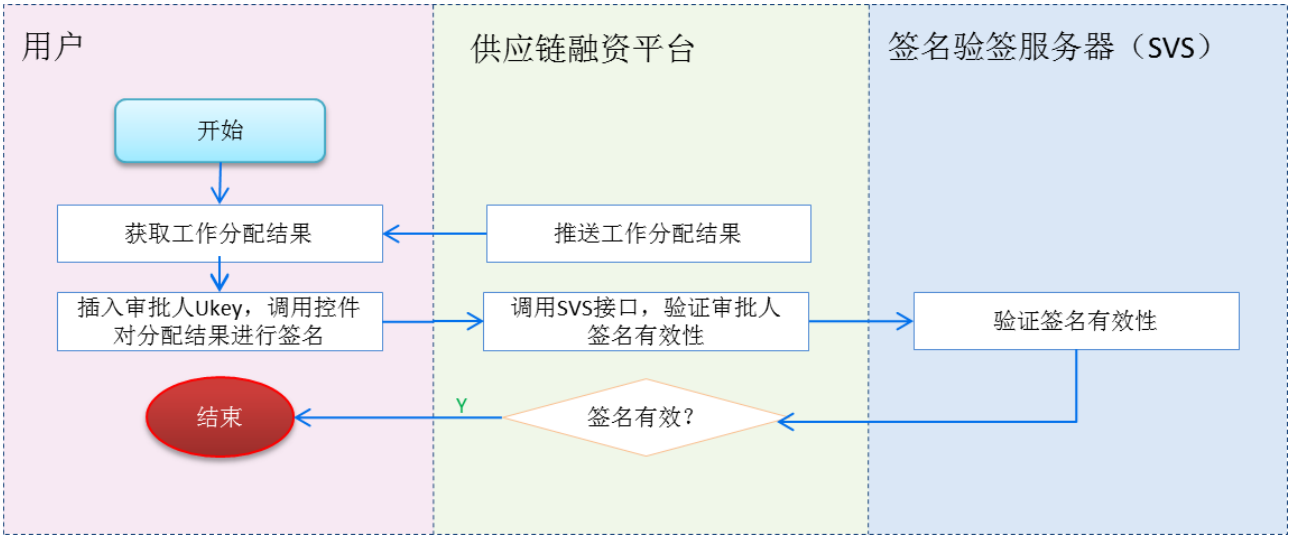
7、交易完成。

4.4 确认

4.4.1 场景说明

平台进行工作分配后，将分配结果及明细推送给前台用户，用户通过 UKey 进行工作确认，确认后有效。此过程需要一级 UKey 确认（审核 UKey），点击“确认”按钮，身份认证通过后同时完成对工作的确认。

4.4.2 业务流程



如上图所示，具体流程如下：

1、用户获取平台推送的工作分配结果；

2、根据系统提示，插入审批人 UKey，调用控件对分配结果信息进行签名，提交到平台；

3、平台调用 SVS 接口，验证审批人签名是否有效；

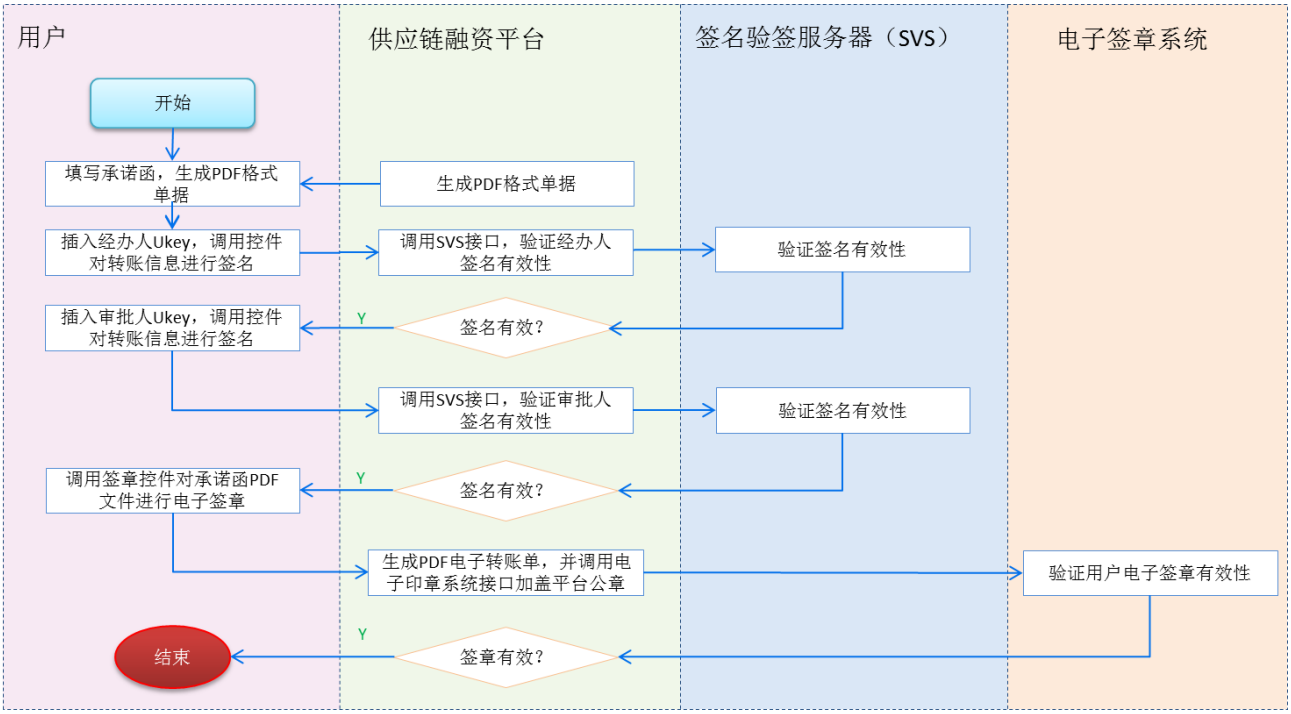
4、如签名有效，则交易完成。

4.5 开立承诺函

4.5.1 场景说明

用户填写承诺函后，生成 PDF 格式的单据，对单据进行两级 UKey 确认。

4.5.2 业务流程



如上图所示，具体流程如下：

1、用户填写承诺函，并提交给平台生成 PDF 格式文件；

2、提示用户插入经办人 UKey，并调用控件对承诺函进行签名，提交给平台；

3、平台调用 SVS 接口，验证经办人的签名是否有效；

4、如果签名有效，则提示用户插入审批人 UKey，并调用控件对承诺函进行签名，提交给平台；

5、平台调用 SVS 接口，验证审批人的签名是否有效；

6、如果签名有效，则并调用审批人 UKey 证书对承诺函进行电子盖章，提交给平台；

7、平台调用电子签章系统接口，验证审批人签章是否有效。

8、交易完成。

4.6 提交申请（如保理申请等）

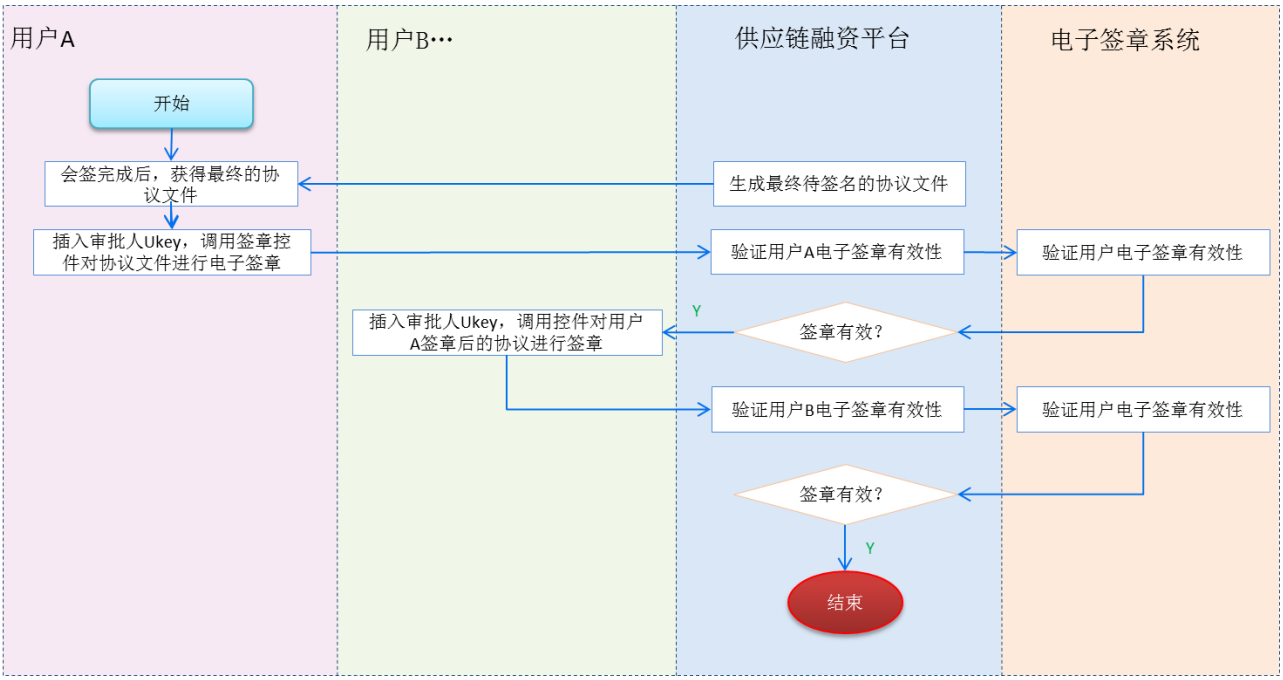
4.6.1 场景说明

情况 1：用户 A 填写申请单，上传附件，整体打包后，进行 UKey 确认，加盖 A 的公章

情况 2：在情况 1 的基础上，加上用户 B 的补充附件，打一个大包加盖 B 的公章，要求同时保留 A 和 B 的公章，并且区分各自公章覆盖的文件范围。

情况 3：在情况 2 的基础上重复一遍，即增加 C 企业。（如再保理项目处理）

4.6.2 业务流程



1、用户 A 获得会签完成后的最终协议文本文件（PDF 格式）；

2、调用用户 A 审批人 UKey 证书对协议进行电子签章，提交给平台；

3、平台调用电子签章系统接口，验证用户 A 审批人签章是否有效；

4、用户 B 获取用户 A 完成签章后的协议文件，并插入审批人 UKey 对协议进行电子签章，提交给平台；

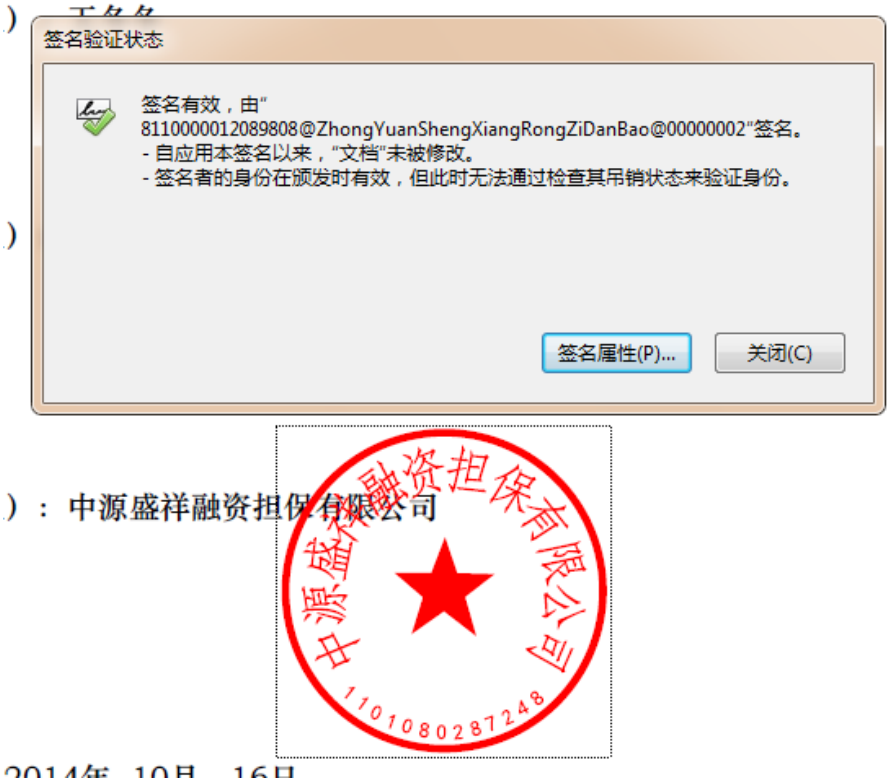
5、平台调用电子签章系统接口，验证用户 B 审批人签章是否有效；

6、交易完成。

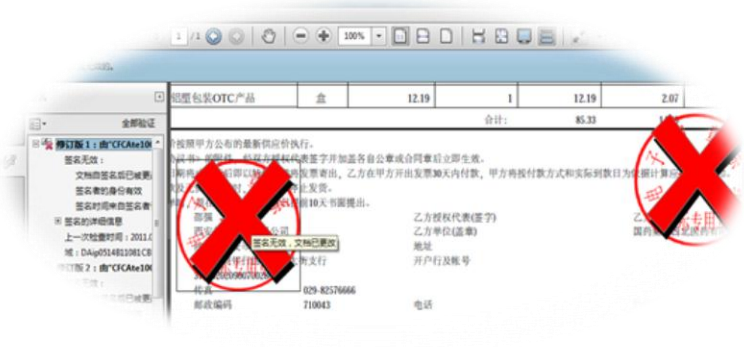
4.7 电子合同展示效果

1、合同示例

2、电子合同验证成功



3、电子合同验证失败



图表 4-3：电子合同展示

4.8 法律保障

4.8.1 电子签名法相关

4.8.1.1 相关概念

电子签名：是指数据电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据。

数据电文：是指以电子、光学、磁或者类似手段生成、发送、接收或者储存的信息。

电子签名的表现形式：

1、附着于电子文件的手写签名的数字化图像，包括采用生物笔迹辨别法所形成的图像。

2、向收件人发出证实发送人身份的密码、计算机口令。

3、采用特定生物技术识别工具，如指纹或者虹膜透视辨别法。

4、使用非对称密码加密系统对电子记录进行加密、解密变换来实现的数字签名。

电子认证服务：是指为电子签名相关各方提供真实性、可靠性验证的公众服务活动。

电子签名人：是指持有电子签名制作数据并以本人身份或者以其所代表的人的名义实施电子签名的人。

电子签名依赖方：是指基于对电子签名认证证书或者电子签名的信赖从事有关活动的人。

电子签名制作数据：是指在电子签名过程中使用的，将电子签名与电子签名人可靠地联系起来的字符、编码等数据。

电子签名验证数据：是指用于验证电子签名的数据，包括代码、口令、算法或者公钥等。

电子签名认证证书：是指可证实电子签名人与电子签名制作数据有联系的数据电文或者其他电子记录。

4.8.1.2 相关规定

数字证书内容：《电子签名法》第二十一条

电子认证服务提供者签发的电子签名认证证书应当准确无误，并应当载明下列内容：

（一）电子认证服务提供者名称；

（二）证书持有人名称；

（三）证书序列号；

（四）证书有效期；

（五）证书持有人的电子签名验证数据；

（六）电子认证服务提供者的电子签名；

（七）国务院信息产业主管部门规定的其他内容。

电子认证服务机构的条件：

《电子认证服务管理办法》第五条 电子认证服务机构，应当具备下列条件：

（一）具有独立的企业法人资格；

（二）从事电子认证服务的专业技术人员、运营管理人员、安全管理人员和客户服务人员不少于三十名；

（三）注册资金不低于人民币三千万元；

（四）具有固定的经营场所和满足电子认证服务要求的物理环境；

（五）具有符合国家有关安全标准的技术和设备；

（六）具有国家密码管理机构同意使用密码的证明文件；

（七）法律、行政法规规定的其他条件。

4.8.1.3 法律效益

立法要解决的是规定安全可靠的电子签名应当达到的标准并赋予其法律效力；而如何达到法定标准，则属于技术问题。

《电子签名法》第十四条：“可靠的电子签名与手写签名或者盖章具有同等法律效力。”

《电子签名法》第十三条

电子签名同时符合下列条件的，视为可靠的电子签名：

（一）电子签名制作数据用于电子签名时，属于电子签名人专有；

（二）签署时电子签名制作数据仅由电子签名人控制；

（三）签署后对电子签名的任何改动能够被发现；

（四）签署后对数据电文内容和形式的任何改动能够被发现。

4.8.2 电子取证服务

CFCA 对使用其证书并进行电子签名的用户提供取证服务。取证内容包括：通过对电子签名验证的方式验证申请人提供的签名结果与数据电文存储地的签名结果是否同一，或者再现数据电文原文；通过审查数字证书签发过程记录，验证电子签名人的真实身份等。

当发生纠纷或需要进行责任鉴定时，就需要进行取证，电子数据具有很多不确定因素，因而取证也与以往的传统取证有所不同，CFCA 能够依据多年的电子认证行业服务经验及以往

的电子取证案例经验，提供权威专业的第三方电子取证服务。

取证服务是以对人员的实名认证为基础，以在应用系统中集成数字签名和证据保全技术为支撑，对人员或机构在业务应用中的操作行为依法进行责任鉴定的服务。

实名认证：取证过程中确定网络行为责任人的业务保障；

数字签名：取证过程中确定行为自发性、数据完整性和结果不可抵赖性的技术保障；

证据保全：取证过程中对数据有效获取、分析和鉴定的技术支撑；

责任鉴定：根据签名验证、主体确认的结果出具责任鉴定报告；

合规性保障：对取证过程中各环节的技术和管理保障措施，以保证取证过程合法、合规，取证结果正确可靠、取证服务风险可控。

5 项目实施

5.1 项目分工

在平台系统中采用 CFCA 数字证书，提高系统使用的安全性，实现用户的有效身份认证和防篡改。本项目目标是建设一套满足需求的证书管理系统、电子印章系统及其他相关产品、服务。

5.2 CFCA 责任

- 组织项目实施团队；
- 与平台系统开发商及利益相关方讨论确认项目需求；
- 提供符合客户需求的软、硬件产品，配合项目集成；
- 配合进行系统测试和上线。

5.3 客户方责任

- 确认项目需求；
- 提供软件测试环境；
- 项目集成，部署安装测试环境；
- 部署安装生产上线环境。

6 附录 A：CFCA 介绍及资质

6.1 CFCA 简介

中金金融认证中心（CFCA）是由中国人民银行牵头，联合各家商业银行成立的公正的、权威的第三方机构，独立于信息传递的任何一方。证书核心密码获得国家商办的认可，证书认证系统获得国家信息安全产品测评认证中心的认证。为了更好地为金融行业服务，2004 年 4 月 CFCA 正式并入银联。CFCA 一直致力于安全基础设施建设和服务提供，为中国金融业、电子商务平台、税务等各种商业应用提供基于 PKI 全面安全解决方案。

目前 CFCA 证书已经在国内外多家商业银行、网上招投标、税务、大型企业以及其他行业得到广泛应用，截止到 2014 年 12 月，累计发放证书超过 8000 万张，占现有市场证书保有量 40%以上。证书应用包括网上银行、网上购物、P2P、网上申报缴税、网上证券、网上保险、网上购销和其他安全业务（OA、MIS）等。

6.2 主要客户

- 银行

中国工商银行、中国农业银行、中国建设银行、中国银行、交通银行、中信实业银行、中国光大银行、中企云链、中国民生银行、广东发展银行、深圳发展银行、兴业银行、浦东发展银行、华一银行（合资银行）、东亚银行（外资银行）、深圳市商业银行、上海银行、天津市商业银行、武汉市商业银行、温州市商业银行、宁波市商业银行、柳州市商业银行、金华市商业银行、威海市商业银行、包头市商业银行、重庆市商业银行、深圳市农村信用合作社联合社、乌鲁木齐商行、恒丰银行、长沙市商业银行等 200 多家银行。

- 证券

港澳证券、蔚深证券、中信证券、山西证券、黄河证券、闽发证券、江门证券、湘财证券、华鑫证券、中富证券、国都证券、金信证券、兴业证券、新华证券、新时代证券、兴安证券等。

- 基金

长城证券；华安、华夏、国泰、长盛、中融、博时、深圳宝盈、社保基金、南方、鹏华、嘉实、大成、长城基金等。

- 其他金融机构

中国人民银行上海分行外汇管理局网上外汇申报系统、中央国债登记系统、中国银联网上信息共享系统和差错处理平台、中国人民银行北京营管部信息平台、厦门卡中心网上认证系统、大连市信用卡中心/大连市信息产业局网上认证系统、北京票据清算中心数据管理系统、深圳金融电子结算中心网上认证系统、中国人民银行武汉分行国库系统、中国人民银行天津分行金融监管中心等。

- 税务、企业集团、财务公司等

北京国税网上申报系统、无锡国税网上申报缴税系统、大连地税网上申报缴税系统；攀钢、鞍钢、中石油、联想、一汽、万向、用友等企业集团内部财务管理系统等。

6.3 公司主要资质

1. 电子认证服务许可证
2. 电子认证服务使用密码许可证
3. 中国国家信息安全测评认证中心测评
4. 软件企业认定证书
5. 高新技术企业认定证书
6. 质量管理体系(ISO9001)认证证书
7. 高新技术企业批准证书
8. 软件企业登记证书（RA）
9. 软件企业登记证书（工具包）
10. 计算机软件著作权登记证书
11. 信息安全服务资质证书
12. 档案管理等级证书
13. 检查机构认可证书
14. 信息安全风险评估服务资质
15. e 盾商标注册-36 类
16. e 盾商标注册-38 类
17. 商用密码产品销售许可证
18. 商用密码产品型号证书--
19. 商用密码产品生产定点单位证书
20. 商用密码产品销售许可证

21. 商用密码产品型号证书--数字认证系统

22. CMMI3 级认证

23. 第三方支付许可

24. WebTrust 国际安全审计认证

6.4 赔付标准

如果由于 CFCA 数字证书自身出现任何安全问题，并通过证明已经给使用 CFCA 数字证书的用户造成了无法挽回的损失，CFCA 将对接受并执行《CFCA 数字证书服务协议》的用户承担相应的赔偿责任：

- CFCA 对企业数字证书用户的赔偿上限为人民币伍拾万元整，即￥500,000.00 元。
- CFCA 对个人数字证书用户的赔偿上限为人民币贰万元整，即￥20,000.00 元。

6.5 CFCA 优势体现

- CA 产品目前在 CFCA 运营使用，可满足金融行业、大型商业、大集团客户性能服务能力
- 具有 300 多家金融及政府大客户及大量电子商务平台的建设和运维电子认证系统的经验
- 拥有完善的三级客服体系，包括 7*24 小时热线支持服务和专业的售后服务团队
- CA 系统外围产品完善，证书应用产品使用广泛、集成简单、易用性强，充分满足项目需求
- 唯一具有赔付标准的 CA 运营公司，唯一具有同城灾备和异地灾备的 CA 运营公司

7 附录 B：方案涉及产品

7.1 证书应用工具包

7.1.1 概述

证书工具包是一套面向应用的开发包。它基于标准的 X.509 数字证书、对称密钥算法、非对称密钥算法，实现了数据保密性、数据防篡改和不可否认性，并将这些功能封装成灵活

易用的开发接口供应用使用。

7.1.2 主要功能

- **数据验签**

支持 PKCS1、PKCS7 等格式的数据签名验签。

- **数据签名**

支持 PKCS1、PKCS7 等格式的数据签名；

支持使用多签名证书进行签名。

- **数据加解密**

支持非对称和对称算法的加解密功能。

- **验证签名证书有效性**

支持验证证书有效期、证书是否合法 CA 颁发和通过 CRL 文件验证签名证书是否被吊销。

7.1.3 产品部署

证书工具包为证书应用套件，分为 PC 端和移动端，直接集成在中企云链平台中，实现证书登录、电子协议电子签名、数据加解密等功能。

7.2 签名验签服务器

7.2.1 概述

CFCA 签名验签服务器是一款硬件产品，实现了身份认证、数据保密性、数据防篡改和不可否认性，并将这些功能封装成灵活易用的开发接口供应用使用。通过软硬一体的形式，提高对数字证书的保护，减轻应用服务器压力，提高签名验签效率。

7.2.2 主要功能

- **数据验签**

支持 PKCS1、PKCS7 等格式的数据签名验签。

- **数据签名**

支持 PKCS1、PKCS7 等格式的数据签名；

支持使用多签名证书进行签名。

- **数据加解密**

支持非对称和对称算法的加解密功能。

- **验证签名证书有效性**

支持验证证书有效期、证书是否合法 CA 颁发和通过 CRL 文件验证签名证书是否被吊销。

- **证书黑名单**

支持通过 HTTP 方式定时自动下载证书黑名单。

还有其他日志和系统管理功能。

7.2.3 产品部署

签名验签服务器部署在平台服务后端，为平台在实现登录、电子协议签署等环节实现强身份认证、资金安全、电子协议合法合规性。

7.3 电子印章系统

7.3.1概述

CFCA 电子签章产品基于 PKI 公钥基础设施，以 PKCS 公钥加密标准为规范，将电子印章和数字签名技术完美结合为一体的应用软件系统，结合具体业务系统，实现数字签名技术在业务系统流程中的应用。解决了业务电子化过程中的公文盖章人身份的确认性、电子公文的信息完整性、公文盖章人的不可抵赖性，并结合传统印章的图章效果，提供给用户一个透明的、安全的、简便的电子印章应用。

7.3.2主要功能

◆ **文档签章**

用户可对编辑完成的文档执行签章操作，对文档进行数字签名，并将用户的印章图片显示到文档的指定位置，生成如同纸质盖章一样的效果，“印章”的显示透明，不影响用户对文档内容的阅读。

◆ **文档验章**

验证签章是否有效，即验证文档内容和签章信息是否被篡改。

◆ **签章信息查看**

用户收到签章文档后，可随时查看签章信息，包括签章是否有效，签章人名称，签章时间，单位名称，印章名称。

◆ **查看签章者证书**

查看签章人证书信息，证书主题名，证书颁发者，证书有效期。

◆ **多人签章**

多人可在同一文档上执行“盖章”操作，文档显示加盖的多个图章。各印章之间彼此独立，后盖的印章不会自动检查之前加盖的印章有效性，也不会影响已有印章的有效性。

7.3.3产品部署

集成于平台中，对 PDF、Web 形式文件进行签章和验证，实现电子合同可视化签章。

7.4 统一认证前置

7.4.1 概述

CFCA 为全国三百多家商业银行提供数字证书认证服务，拥有海量的网银证书及可靠用户信息数据基础。在此基础上，CFCA 推出统一的身份认证服务，用户只要拥有 CFCA 颁发的数字证书，即可以通过网银证书在互联网上鉴别其真实身份，方便开展各种互联网金融业务。

7.4.2 主要功能

统一认证平台提供的基本服务有如下两种：

1、证书校验服务：根据证书序列号和颁发者校验证书是否存在，检查证书状态；

2、订户身份信息校验服务：根据序列号、颁发者校验用户信息是否匹配；

目前平台的主要特点如下：

1、安全性：数据可靠可信；基于成熟的 PKI 体系，保证业务系统访问安全及业务安全；

2、便捷性：用户使用已有的网银证书，不用临柜办理业务，可以办理多种互联网金融业务；

3、标准性：提供标准的公共服务接口；

4、合规性：符合《中国人民共和国电子签名法》的要求。使用统一认证平台进行远程身

份认证，可以提升业务系统身份认证强度，满足人行的强实名认证要求。

7.4.3 产品部署

统一认证前置系统部署在中企云链，平台提交用户身份信息和证书信息由统一认证前置访问 CFCA 统一认证平台实现企业身份的实名验证。

7.5 密码安全控件

7.5.1 概述

密码控件是为了保障客户帐户的信息安全，保护用户输入的信息，防止木马程序截取账户密码、银行卡信息等键盘记录。

7.5.2 主要功能

密码控件主要功能如下：

- 获得密码长度设置要求：通过方法获得密码是否符合设置的要求。
- 获得密码字符匹配：通过方法获得密码所使用字符是否符合正则表达式。
- 获得客户端的随机数：由方法获得客户端生成的随机数。
- 获取密码的加密结果：通过调用方法获得密码的 3DES 加密结果。
- 设置相关规则：包含密码长度、密码输出类型、生成的随机数等。
- 敏感信息防护：能够防范攻击者通过用户态程序挂钩键盘消息。
- 自身安全性：具备高强度逆向分析篡改防护功能，能够防范攻击者通过反编译。

7.5.3 产品部署

PC 端产品用于 PC 端网页集成，移动端产品用于移动终端 APP 集成，实现敏感信息的加密。

7.6 SSL 安全网关

7.6.1 概述

CFCA 数据安全网关是一款保障网络通信安全的服务器系统，它能提供客户端浏览器和 Web 服务器之间的身份认证和安全通信，从而在网络交易过程中保证交易安全和实现访问控制。

7.6.2 产品功能

- HTTPS 代理：在客户端浏览器和 Web 服务器之间建立基于数字证书的高强度为 128 位加密安全连接。
- HTTP 代理：安全网关起到转发客户端请求的功能。
- 代理多个应用服务器：数据安全网关通过使用 SSL 通信方式可以同时保护多个应用服务器。
- 身份认证：客户端验证服务器证书；服务器对客户端证书的验证有两种模式：需要客户端证书和不需要客户端证书
- 黑名单验证：数据安全网关可以通过 CRL 验证客户端证书的有效性。

7.6.3 使用场景

SSL 安全网关部署在平台服务前端，为用户端页面提供 SSL 安全通道加速功能，确保用户页面传输至平台服务端数据的安全性。

7.7 时间戳服务

7.7.1概述

在电子借贷协议中，时间是十分重要的信息。文件签署的日期和签名一样均是十分重要的防止文件被伪造和篡改的关键性内容。CFCA 作为一个权威的、可信赖的、公正的第三方，其时间戳服务就是将经过 CA 签名的一个可信赖的日期和时间与特定电子数据绑定在一起，为电子合同提供可信的时间证明。

7.7.2主要功能

在时间戳服务中，包括如下两部分，每个部分都是获取时间戳服务的关键。

- **标准时间获取**

时间源为国家授时中心的标准时间，为保证电子病历时间的准确性和不受干扰，我们将采用 GPS 卫星授时设备来获取标准时间。

- **时间戳提取**

提供时间戳提取接口，获得时间值

7.7.3服务使用

由中企云链平台远程访问 CFCA 时间戳服务，以确保操作痕迹记录都采用了相同的时间基准，保证电子借贷协议是经过加盖时间戳的。