ICS 03.060
A 11

中国互联网金融协会标准

T/NIFA X—XXXX

互联网金融　个体网络借贷
电子合同安全规范

Internet finance — P2P lending — Security specification for electronic contract

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上

XXXX-XX-XX 发布　　XXXX-XX-XX 实施

中国互联网金融协会　　发 布

目　　次

前　言

本标准按照GB/T 1.1—2009《标准化工作导则 第1部分：标准的结构和编写》和GB/T 20004.1-2016《团体标准化 第1部分：良好行为指南》给出的规则起草。

本标准由中国互联网金融协会提出。

本标准由中国互联网金融协会归口。

本标准起草单位：

本标准主要起草人：

引　　言

为保证互联网金融个体网络借贷行业电子合同在线订立的安全性和合法性，互联网金融网络借贷信息中介机构需使用可靠的电子签名，订立后的电子合同应委托电子合同第三方存储服务商进行存储。为规范电子合同订立时采用电子签名技术的各项安全要求，提高电子合同订立的安全性和证据效力，特制定本标准。

本标准严格遵循《中华人民共和国合同法》《中华人民共和国电子签名法》《电子认证服务管理办法》和《网络借贷信息中介机构业务活动管理暂行办法》的相关规定，同时根据互联网金融行业的特点，参考金融行业相关标准规范而制定。

行业主管部门另有规定的，遵循主管部门的相关规定。

互联网金融 个体网络借贷 电子合同安全规范

1 范围

本标准提供了互联网金融网络借贷信息中介从业机构（以下称“从业机构”）在开展网络借贷信息中介业务活动中，当事人在中华人民共和国境内通过互联网在线订立电子合同时采用可靠的电子签名，保证订立后的电子合同满足防篡改、抗抵赖性等各项安全要求，以提高通过此种方式订立的电子合同的安全性和证据效力。

本标准适用于指导从业机构开展网络借贷信息中介业务活动时使用电子签名技术对电子合同进行在线订立，并将订立后的电子合同进行第三方存储，进一步满足互联网金融个体网络借贷行业安全性及合法合规性要求。

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。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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。

中华人民共和国电子签名法

GB/T 20520—2006 信息安全技术 公钥基础设施 时间戳规范

GB/T 20988—2007 系统灾难恢复规范

GB 50174—2017 数据中心设计规范

JR/T 0118—2015 金融电子认证规范

SB/T 11009—2013 电子合同在线订立流程规范

T/NIFA 1—2017 互联网金融 信息披露 个体网络借贷

公通字[2007]第43号 信息安全等级保护管理办法

3 术语与定义

T/NIFA 1—2017中界定的术语和定义以及下列术语和定义适用于本文件。

3.1

实名核验 identity proofing

验证充分信息以确认实体声明身份的过程。

3.2

电子合同 electronic contract

平等主体的自然人、法人、其他组织之间以数据电文为载体，并利用电子通信手段设立、变更、终止民事权利义务关系的协议。

3.3

电子合同缔约人 electronic contract party

使用电子合同订立系统的合同当事人，简称合同缔约人。

3.4

电子认证 certificate authentication
基于 PKI 的数字签名认证技术。

3.5

电子认证服务 electronic certification service
为电子签名相关各方提供真实性、可靠性验证的活动。

3.6

身份证网证 electronic identity authentication certificate
居民身份证网上功能开通凭证。

3.7

电子合同订立系统 signing system of electronic contract
电子合同订立系统是指具备缔约人身份认证、谈判磋商、合同电子签名、合同存储与调用等功能以实现在线订立电子合同及处理的信息系统。
第三方电子合同订立系统是独立于从业机构的第三方主体运营的电子合同订立系统。

3.8

数字证书 digital certificate
由证书认证机构签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息的一种数据文件。按类别可分为个人证书、机构证书和设备证书，按用途可分为签名证书和加密证书。

3.9

电子合同第三方存储服务商 third-party storage service provider for electronic contract
独立于电子合同缔约各方和从业机构，能提供电子合同信息保存的服务机构，简称第三方存储服务商。它可以应合同缔约一方或多方的请求对合同订立过程提供多种形式的存储服务并提供信息完整性和准确性证明。
第三方存储服务商不应是从业机构的关联公司、从业机构内部的隔离系统或由第三方部署在从业机构内部的私有云等。

3.10

时间戳 time stamp
使用数字签名技术产生的数据，签名的对象包括了原始文件信息、签名参数、签名时间等信息。时间戳机构对此对象进行数字签名产生时间戳，以证明原始文件在签名时间之前已经存在。

3.11

时间戳机构 time stamp authority
用来产生和管理时间戳的权威机构。

3.12

可信时间 trusted time

准确的、值得信赖的当前时间值，这个时间值的来源应是高度权威的。

4 缩略语

下列缩略语适用于本标准：

PKI	Public Key Infrastructure	公钥基础设施
APP	Application	应用程序
OV	Organization Validation	组织机构认证
EV	Extended Validation	扩展认证
SSL	Secure Sockets Layer	安全套接层

5 电子签名合法性要求

电子合同的订立应满足《中华人民共和国电子签名法》的规定。

a）电子签名人真实身份的标识

电子签名人是创建可靠电子签名的实体，可以是自然人或单位机构授权的代表人。对电子签名人身份的正确标识是可靠电子签名的根本。

b）电子认证服务机构

电子认证服务机构是指帮助电子签名人和依赖方建立信任关系的实体，即证明电子签名制作数据和电子签名人真实身份的关联关系。

在可靠电子签名体系中，标识电子签名人真实身份的数字证书应由第三方电子认证服务机构进行颁发，电子认证服务机构应取得工业和信息化部颁发的《电子认证服务许可证》，并符合工业和信息化部的各项管理要求和在工业和信息化部备案的《电子认证业务规则》。信息系统安全等级保护应为三级或更高级别。

6 电子合同订立

6.1 概述

借款人、出借人以及从业机构在平台从事投融资活动时，为了保障商务活动各方主体的权益，应订立有法律效力的电子合同。从业机构应提供渠道供借款人和出借人查看、下载已订立的电子合同。服务渠道包括但不限于网站、移动 APP 应用、社交媒体公众号或服务号等。

借款人和出借人应先通过实名核验，由电子认证服务机构为其签发数字证书，借款人和出借人使用数字证书对电子合同进行签名，电子签名依赖方使用电子签名验证数据进行电子合同完整性验证，并且确认借款人和出借人的真实身份，防止借款人和出借人抵赖订立电子合同的行为。

6.2 实名核验

6.2.1 实名核验要求

借款人、出借人登录平台，应提交真实、完整和准确的个人或企业身份信息，平台应对平台上产生投融资活动的借款人、出借人的身份信息进行审核，只有实名核验通过的个人或企业，才能在平台进行投融资活动。

实名核验包含对借款人和出借人提供的有效证件真实性、一致性、意愿真实性三方面进行核验。平台可根据平台自身的风控制度自主选择实名核验的方式。

6.2.2 个人实名核验

平台在对个人进行实名核验时可采用的方式包含以下几种：

a) 线下核验：包括对个人有效证件的现场审核，个人生物特征信息的采集及比对核验，进行人证合一的确认；
b) 线上核验：核验信息包括姓名、身份证号码或身份证网证、手机号码或银行卡号（至少包括姓名、身份证号码和身份证网证中的一种），应利用政府权威部门的数据库或取得政府权威部门授权或认可的数据库等，并采用生物特征识别技术或其他安全有效的技术手段进行人证合一的确认；也可通过电子认证服务机构颁发的数字证书进行实名核验；
c) 其他经过认可的，可保证个人有效证件真实性、一致性及意愿真实性的实名核验方式。

6.2.3 企业实名核验

平台在对企业进行实名核验时可采用的方式包含以下几种：

a) 线下核验：包括对企业有效证件，企业资料，经办人的企业合法授权文件的现场审核，以及经办人的个人实名核验；
b) 线上核验：核验信息包括企业名称、工商登记号、组织机构代码（或统一社会信用代码）、法人代表姓名和法人代表身份证号码或身份证网证（至少包括企业名称、工商注册号或统一社会信用代码），应采用经办人个人实名核验，以及企业核心隐私数据的核验，例如对公银行打款、开具指定金额发票等核验方式；也可通过电子认证服务机构颁发的数字证书进行实名核验；
c) 其他经过认可的，可保证企业有效证件真实性、一致性及意愿真实性的实名核验方式。

6.3 数字证书申请

6.3.1 数字证书申请流程

借款人、出借人应在平台上通过实名核验，才能申请数字证书。

6.3.2 个人数字证书申请的有效身份证件

在证书申请时对个人身份进行鉴别时，应符合 JR/T 0118-2015 针对个人有效身份证件的要求。

6.3.3 企业数字证书申请的有效证件

在证书申请时对机构身份进行鉴别时，应符合 JR/T 0118-2015 针对企业有效身份证件的要求。

6.4 密码算法及密码产品要求

电子合同订立系统所涉及的密码算法可包括但不限于：杂凑算法、非对称密码算法、对称密码算法等，所有算法应是国家密码主管部门认可的算法。

电子合同订立系统采用的密码模块或密码产品应具有国家密码管理局颁发的商用密码产品型号资质证书。

6.5 电子签名制作数据使用方式

电子合同订立系统涉及的电子签名制作数据的使用方式应满足《中华人民共和国电子签名法》中关于可靠的电子签名的要求。

6.6 时间戳要求

电子合同采用的可信时间戳应满足如下要求：

a) 从业机构或其合作的第三方电子合同订立系统服务商应确保合同具备可信时间戳要素，满足防篡改要求；

b) 时间戳要求应满足GB/T 20520-2006中规定的要求。

6.7 电子合同订立系统要求

6.7.1 概述

从业机构可自建电子合同订立系统，也可使用第三方电子合同订立系统订立电子合同。电子合同订立系统应独立于平台。

6.7.2 资质要求

电子合同订立系统应具备公安部信息安全等级保护三级或者更高级别认证。

电子合同订立系统部署在公有云时，云服务应通过工业和信息化部的可信云服务认证。

电子合同订立系统的服务商应具备 ISO 27001 认证。

6.7.3 真实身份标识

从业机构采用第三方电子合同订立系统的，第三方电子合同订立系统应使用OV或EV SSL网站认证证书等手段标识网站的真实性，并有效保护交易信息的安全。

6.7.4 业务持续性保障

a) 应部署在符合GB 50174-2017要求的A级数据中心机房；

b) 应建立或使用与其业务规模相匹配的灾备系统设施，系统的灾难恢复能力应满足GB/T 20988-2007的第五级要求，实时数据传输及完整设备支持，保证业务持续性及应急响应；

c) 应提供7*24小时服务，并提供7*24小时服务热线，全年服务可用率应达到99.95%及以上。

6.7.5 通讯安全

平台和电子合同订立系统之间的数据在公网传输时应采用数据加密技术实现机密性保护，保证数据传输的安全性。

6.7.6 终止或转移服务

从业机构使用第三方电子合同订立系统的，应与其服务商约定履行如下义务：

a) 第三方电子合同订立系统服务商不能继续提供服务时，应当在终止或转移服务九十日前以书面形式告知从业机构；

b) 第三方电子合同订立系统服务商应向从业机构提供双方认可的电子合同数据迁移方案并提供技术支持，保证从业机构电子合同数据迁移过程的机密性、完整性、可用性。

6.7.7 安全评估与监管

从业机构应依据《信息安全等级保护管理办法》中要求，对电子合同订立系统定期开展等级保护测评，测评应由具备等级保护测评资质的信息安全测评认证机构进行。

从业机构使用第三方电子合同订立系统的，第三方电子合同订立系统服务商应公示业务规则，接受主管部门的定期检查，并将信息安全测评认证结果向使用其第三方电子合同订立系统服务的从业机构、借款人和出借人公开披露。

第三方电子合同订立系统服务商应配合从业机构向监管部门或行业自律组织完成报备等合规工作。

6.7.8 数据安全

数据安全主要包括数据存储安全、授权访问控制、隐私保护和数据备份。

a) 平台和电子合同订立系统应采取安全措施，确保电子合同不泄露，对电子合同进行加密存储；
b) 平台和电子合同订立系统应具有授权访问控制功能，借款人和出借人只有通过实名核验后，才可查看、下载本人已订立的电子合同；
c) 电子合同订立系统应对电子合同进行备份并加密存储，并完整记录用户操作日志以备审计。第三方电子合同订立系统服务商应对电子合同信息严格保密，并建立健全信息保护制度，加强内部人员安全管理，确保不泄露电子合同信息。

6.8 电子签名验证

从业机构应对借款人和出借人提交的电子签名进行验证，以保证电子合同的完整性和抗抵赖性，电子签名验证应满足如下要求：

a) 验证用户数字证书的有效性；
b) 验证数字签名的有效性；
c) 验证签名所使用的签名算法是否符合要求；
d) 验证签名所使用的数据摘要算法是否符合要求；
e) 验证产生签名的数字证书与用户的关联关系。

电子合同订立系统应具有在线校验电子合同的功能，验证签名者的身份、数字证书、时间戳的有效性。如果合同内容或签名被篡改，应提示文档被篡改、失效。

6.9 从业机构真实身份标识

平台应使用 OV 或 EV SSL 网站认证证书等手段标识交易网站的真实性，并有效保护交易信息的安全。

6.10 从业机构安全评估与监管

从业机构应记录并留存借款人和出借人的合同记录，留存期限为自合同到期日起 5 年，对于已有法律、规章规定电子合同保存期的，电子合同保存期限应与该保存期一致。

从业机构应聘请有资质的信息安全测评认证机构定期对信息安全实施测评认证，向出借人与借款人等披露测评认证结果，且定期开展安全评估，接受国家和行业主管部门的信息安全检查和审计。

7 电子合同存储

7.1 概述

电子合同应通过电子合同第三方存储服务商进行存储与备份。

电子合同保存期限应自合同到期日起 5 年，对于已有法律、规章规定电子合同保存期的，电子合同保存期限应与该保存期一致。

7.2 密码算法及密码产品要求

电子合同第三方存储系统所涉及的密码算法可包括但不限于：杂凑算法、非对称密码算法、对称密

码算法等，所有算法应是国家密码主管部门认可的算法。

电子合同第三方存储系统采用的密码模块或密码产品应具有国家密码管理局颁发的商用密码产品型号资质证书。

7.3 资质要求

电子合同第三方存储系统应具备公安部信息安全等级保护三级或者更高级别认证。

电子合同第三方存储系统部署在公有云时，云服务应通过工业和信息化部的可信云服务认证。

电子合同第三方存储服务商应具备 ISO 27001 认证。

7.4 真实身份标识

电子合同第三方存储系统应使用OV或EV SSL网站认证证书等手段标识网站的真实性，并有效保护交易信息的安全。

7.5 业务持续性保障

a) 应部署在符合GB 50174-2017要求的A级数据中心机房；
b) 应建立或使用与其业务规模相匹配的灾备系统设施，系统的灾难恢复能力应满足GB/T 20988-2007的第五级要求，实时数据传输及完整设备支持，保证业务持续性及应急响应；
c) 应提供7*24小时服务，并提供7*24小时服务热线，全年服务可用率应达到99.95%及以上。

7.6 通讯安全

电子合同订立系统和电子合同第三方存储系统之间的数据在公网传输时应采用数据加密技术实现机密性保护，保证数据传输的安全性。

7.7 终止或转移服务

从业机构应与电子合同第三方存储服务商约定履行如下义务：

a) 电子合同第三方存储服务商不能继续提供服务时，应当在终止或转移服务九十日前以书面形式告知从业机构；
b) 电子合同第三方存储服务商应向从业机构提供双方认可的电子合同数据迁移方案和技术支持。

7.8 安全评估与监管

电子合同第三方存储系统应由有资质的信息安全测评认证机构定期对信息安全实施测评认证，并向使用其服务的从业机构、借款人和出借人披露测评认证结果。

电子合同第三方存储服务商应配合从业机构完成监管部门或行业自律组织要求的报备、检查等合规工作。有监管要求时由国家级行业自律组织使用解密密钥解密原文。

7.9 数据安全

数据安全主要包括数据存储安全和隐私保护。

a) 平台和电子合同第三方存储系统应采取安全措施，确保电子合同不泄露，对电子合同进行加密存储。电子合同的加密密钥和解密密钥应由国家级行业自律组织管理，从业机构应使用上述加密密钥将电子合同加密存储在电子合同第三方存储系统，密钥管理应符合国家密码管理部门及行业主管部门要求；
b) 电子合同第三方存储系统应完整记录用户操作日志以备审计。电子合同第三方存储服务商应对电子合同信息严格保密，并建立健全信息保护制度，加强内部人员安全管理，确保不泄露电子合同信息。

8 司法举证要求

当发生平台跑路等恶性事件或借款人、出借人在平台产生纠纷时，相关当事方（包括但不限于从业机构、第三方电子合同订立系统服务商、电子合同第三方存储服务商）具有协助举证方（包括但不限于公检法机构、借款人、出借人）进行举证的义务。证据证明包括但不限于：

a） 从业机构提供订立的电子合同原文，借款人、出借人在平台的实名核验、支付、投资记录、还款记录等证据，从业机构依据《网络安全法》对公民个人信息安全保护以及告知义务的履行证明文件，从业机构对接的支付机构或存管银行提供资金流水记录等证据；

b） 第三方电子合同订立系统服务商和电子合同第三方存储服务商宜与仲裁机构或司法鉴定机构等电子证据机构对接，如有司法举证的需求，合作的电子证据机构应出具鉴定报告；

c） 电子认证服务机构出具数字证书验证报告，证明证书及电子签名的有效性；

d） 电子签名人委托他人代为实施签名行为时，从业机构或第三方电子合同订立系统服务商提供电子签名制作数据由电子签名人控制的证据，包括调用电子签名制作数据的时间和方式、电子签名人位置、IP地址、授权及认证方式、授权及认证记录等；

e） 有司法举证要求时由国家级行业自律组织使用解密密钥解密原文；

f） 司法机构要求配合提供的其他相关证据。

参 考 文 献

[1] 中华人民共和国合同法
[2] 中华人民共和国网络安全法
[3] 电子认证服务管理办法
[4] 电子认证服务密码管理办法
[5] 国务院[1999]第273号 商用密码管理条例
[6] 银发[2015]第221号 关于促进互联网金融健康发展的指导意见
[7] 银发[2015]第392号 中国人民银行关于改进个人银行账户服务加强账户管理的通知
[8] 银监会令[2016]第1号 网络借贷信息中介机构业务活动管理暂行办法
[9] GB/T 20518-2006 信息安全技术 公钥基础设施 数字证书格式
[10]GB/T 25064-2010 信息安全技术 公钥基础设施 电子签名格式规范