电子签名社会信任的模式形成、风险挑战与应对策略

The Formation Models, Risk Challenges, and Response Strategies of Social Trust for Electronic Signatures

汪琛 /WANG Chen　　李正风 /LI Zhengfeng

（清华大学社会科学学院、科技与社会研究中心，北京，100084）
(School of Social Sciences; Research Center for Science, Technology and Society, Tsinghua University, Beijing, 100084)

摘　要：作为数字化基础设施的关键组成技术之一，电子签名通过重构传统缔约形式，有效助力了社会与经济活动向无纸化、即时化、智能化的转型跃迁。在这一过程中，电子签名社会信体系的构建呈现渐进式多维演进特征，历经契约信任、技术信任到数字信任的三阶段迭代融合。当前，电子签名的可信任性面临来自技术安全、法律合规、社会认可及伦理道德考量等方面的系统性挑战。为此，建议在完善电子签名管理体制机制的基础上，进一步优化相关法规和标准化细则，有效平衡开放实践与严格监管之间的关系，并通过科学知识的普及教育与法律规范的广泛宣传，提升公众对电子签名技术的认知水平，确保电子签名技术社会公信力的稳步提增。

关键词：电子签名　社会信任　数字化转型　技术治理

Abstract: As a critical component of digital infrastructure, electronic signatures have effectively facilitated the transformation of socioeconomic activities toward paperless, real-time, and intelligent operations by restructuring traditional contracting processes. Throughout this process, the establishment of social trust in electronic signatures has demonstrated characteristics of progressive multi-dimensional evolution, undergoing three developmental phases: contractual trust, technological trust, and digital trust, with iterative integration across these stages. Currently, the trustworthiness of electronic signatures faces systemic challenges encompassing technical security, legal compliance, social acceptance, and ethical considerations. To address these issues, it is recommended to refine relevant regulations and standardization protocols based on improving the management framework of electronic signature systems. This approach should effectively balance open innovation with rigorous supervision while enhancing public understanding of electronic signature technology through comprehensive scientific education initiatives and extensive dissemination of legal norms. Such measures will ensure the steady enhancement of social credibility in electronic signature technology.

Key Words: Electronic signature; Social trust; Digital transition; Technology governance

中图分类号：P209; B82　DOI: 10.15994/j.1000–0763.2025.09.011　CSTR: 32281.14.jdn.2025.09.011

从早期文明至今，人类始终在寻求物质载体与主体意志的最优联结方式。早在汉谟拉比法典时期，即有通过压印戒指图案建立责任关联，中国古代也有“画指为信”将指纹的生物

基金项目：工业与信息化部指导性软课题“基于电子签名的社会信任体系研究”（项目编号：GXZK2024-55）；中国博士后科学基金面上资助“人工智能伦理实证研究的哲学审视”（项目编号：2024M751746）；国家资助博士后研究人员计划“基于社会–技术互构论的医疗大模型伦理治理研究”（项目编号：GZC20231384）。

收稿日期：2024 年 11 月 24 日

作者简介：汪　琛（1996–）男，安徽合肥人，清华大学社会科学学院博士后、清华大学科学与社会研究中心助理研究员，研究方向为科技治理、科技伦理。Email: chen0522@mail.ustc.edu.cn

李正风（1963–）男，安徽宿县人，清华大学社会科学学院、科学与社会研究中心教授，研究方向为科技哲学、科技伦理。Email: Lizhf@tsinghua.edu.cn

学特征转化为信用凭证。电子签名作为数字时代重要的认证技术，凭借其高效、便捷、环保等优势，逐渐在合同签署、文件认证、交易确认等多个领域取代了传统纸质签名，成为现代社会与商业活动不可或缺的一部分。[1]所谓电子签名①，本质是一种认证技术，[2]是指通过密码技术对数据电文进行加密处理，以电子形式确认签署者身份及签署意愿的一种技术手段。然而，尽管电子签名技术在当前已然实现了商用规模化，但其赖以存续的社会信任体系正遭遇着多重解构危机。这种信任体系的剧烈震荡不仅制约着技术效能的充分释放，更可能通过信任传导机制从技术采纳层面向数字经济生态基础加速扩散，在数字化契约社会的建构进程中埋下风险隐患。

鉴于此，本文通过梳理电子签名自70年代诞生以来的信任模式演化与迭代进程，分析电子签名技术可能遭遇的社会信任危机与挑战。在此基础上，提出优化电子签名社会公信力的可行策略，旨在为我国数字化转型以及在认证服务领域的创新发展提供理论参考。

一、电子签名社会信任模式的形成条件与契机

1. 契约信任：纸质笔签的电子化载体

在传统社会中，信任机制的构建本质是通过道德自律形成的信誉资本、社会关系衍生的监督机制以及仪式化缔约行为等交织的纽带结构。正是在这种立体化的信任网格中，签名逐步演变为具备法律要式的认证符号，其物理层面的笔迹特征，与主体意志紧密相连，形成了一种不可分割的具身化关联和人格延伸。当步入信息化时代，电子签名通过信息化手段模拟和续载了纸质签名的法律效力和契约精神。使得在现代社会中，即便身处不同的物理空间和时间点，人们也能便捷地完成合同签署和交易确认。尽管电子签名呈现形式和技术手段，与传统纸质签名大相径庭，但在核心功能上，两者并无实质性差异，都作为具有法律效力的形式载体，用于证明签署行为的发生，确认签署者对文件内容的认可和承担相应责任。由此可见，电子签名更多是作为纸质签名在信息化领域的延申，除了媒介形式、验证方式、应用场景等表观因素之外，并没有改变签名作为法律行为和承诺确认的本质属性。

电子签名之所以能够续载传统纸质签名的契约内核，离不开强制性的制度支撑。1995年，美国犹他州颁布的《数字签名法案》，开创了电子认证法律制度的先河。该法案认可经认证机构（Certificate Authority, CA）签发的电子签名，具有与传统手写签名同等的法律效力，还明确规定CA需经州政府许可，并制定了密钥管理、记录保存等规则，尝试将传统公证机制移植至数字空间，以构建可信任的电子交易环境。2001年，联合国通过《电子签名示范法》，为各国电子签名立法提供示范参考。与此同期，世界范围内的电子签名立法开始加速，如欧盟《电子签名指令》、美国《全球暨全美商业电子签章法》、中国《中华人民共和国电子签名法》。这些法律法规对电子签名可信任性的确认，从根本上赋予了电子签名合法的效力身份，为电子签名在各种商业和法律活动中的应用提供了可用的法理依据，让人们能够放心地使用电子签名进行各类事务。

与此同时，技术标准化也在电子签名契约信任的建构过程中发挥了关键作用。主要包括两类：一是电子签名的技术标准化，1993年美国国家标准与技术研究院发布了电子签名算法（Digital Signature Algorithm, DSA），并被纳入联邦信息处理标准《数字签名标准》（Digital Signature Standard, DSS），为基于公钥密码学原理创建和验证数字签名提供了标准参照，随后还出现了国际电信联盟电信标准化部门、国际标准化组织ISO/IEC14888以及中国《电子签名格式规范》等，为电子签名方案提供了附加

①根据《中华人民共和国电子签名法》第二条的定义，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。

指南。二是明确电子签名的类型分级，如2014年欧盟颁布的《电子身份识别、认证和信任》，将电子签名分为简单、高级和合格三个级别，对不同级别的技术要求和法律地位等进行了明确规定，确保了电子签名在欧盟内部的合法性和互认性。这些具化的技术标准，从安全可控、规范统一、通用兼容等维度共同发力，与电子签名法律法规双向赋能、协同共进，加速了电子签名的合规化应用，合力巩固电子签名在现代社会的契约信任基础。

2. 技术信任：契约基石上的技术赋能

在新一代密码学理论的革新与加成下，电子签名社会信任的模式构建逐渐从传统的人际契约模式转向为去人格化的技术信任模式。20世纪70年代前，对称密钥算法是密码系统的主流①，这种算法的特点是加解密过程使用同一个密钥，因此密钥必须严格保密，且只在通信双方间共享。1976年，惠特菲尔德·迪菲（Whitfield Diffie）和马丁·赫尔曼（Martin Hellman）在提出了Diffie-Hellman密钥交换算法，[3]标志电子签名的早期诞生。1977年，麻省理工学院的罗纳德·里维斯特（Ronald Rivest）、阿迪·萨莫尔（Adi Shamir）和伦纳德·阿德曼（Leonard Adleman）②提出了可用于生成原始电子签名的RSA（Rivest-Shamir-Adleman）算法，[4]其安全性依赖于大整数因式分解。因此RSA算法加密安全性较高，成为电子签名技术可信任的重要算法支柱，并在20世纪80年代被集成到早期的电子签名系统中。

20世纪80年代，公民自由团体开始关注政府的监控权力与隐私权问题，密码学开始从军事技术转变为民主社会的数字“盾牌”，并逐渐演变为1980年代的“密码朋克”（Crypto-punk）运动。[5]这期间，最具有代表性的事件是“极佳隐私”（Pretty Good Privacy, PGP）安全通信的协议工具诞生：[6]1991年，菲尔·齐默曼（Phil Zimmermann）开发了名为PGP的加密通讯协议③，并提供该程序连同其源代码以供下载，这是第一个广泛使用的实现公钥加密的程序，使得普通用户也能保护自己的通信隐私④。以此为起点，密码学逐渐从情报机构的专属工具，转变为支撑信息时代的基础技术架构。

这一时期，电子签名以密码学算法为技术内核，在数字证书、公钥基础设施（Public Key Infrastructure, PKI）等要素构成的全链加持下，将物理性的签名行为转化为技术性的数学问题。不仅承接了传统的契约信任，更通过技术特性延伸了信任的时空边界，将纸质签名时代的“物理实体+制度威慑”型信任转化为算法主导的“工业标准化”模式，实现了电子签名的社会信任逻辑从制度性的“对契约的信任”升级为技术性的“对客观数学规则的信任”。这种技术信任模式，本质是将对技术的信任锚定在可编程的数学知识确定性之上。在技术信任模式的驱动下，用户和组织越来越倾向于依靠技术解决方案来确保签名的可信任性。随着对技术依赖的程度加深，以及电子签名的交互友好型和验证便捷性能力的提升，进一步加快塑造和巩固了用户对电子签名技术可信任性的正向认识。

3. 数字信任：电子签名的数智化进阶

面对日益复杂化的数字生态，既往“技术工具+律法制度”的信任模式，逐渐难以适应数字时代的社会信任需求新变化。在此背景下，电子签名逐渐从孤立存在的单簇技术，开始深度融入数字业务流程之中，成为数字生态链接

①英国著名作家、数学家刘易斯·卡罗尔（Lewis Carroll）在其短文“The Alphabet Cipher”中，将“维吉尼亚密码”称之其是“牢不可破的”。但维吉尼亚密码一直饱受学界和学者诟病，并最终于1863年被德国密码学家弗里德里希·卡西斯基（Friedrich Kasiski）完全破解，参见：https://crypto.interactive-maths.com/vigenegravere-cipher.html。

②三位发明人2002年共同获得图灵奖，以表彰RSA算法及其在实践中对密码学的影响。

③菲尔·齐默曼在1999年撰写了一份博文“我为什么写PGP”（Why I Wrote PGP），阐述了PGP的创立愿景是“使人们能够将自己的隐私掌握在自己手中”，https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html。

④1993年，齐默曼因PGP的广泛传播被美国政府以违反《武器出口管制法（Arms Export Control Act）》起诉（在众多开源团体和用户的坚决维护下，最终撤销指控），其本人也因其在密码学领域的开创性工作而获得了诸多重量级的技术嘉奖和人道主义奖项。详见美国科普作家和媒体理论家史蒂文·约翰逊（Steven Johnson）的博文“加密战争：Philip Zimmermann如何为我们的隐私权而战”，https://hiddenheroes.netguru.com/philip-zimmermann。

的核心节点和关键纽带。电子签名的数智化进阶，标志其从以往简单的电子化签名形式，朝着更高阶的多技术融合与深度数字化形态加速演变。在虚拟的数字环境中，通过复杂的算法和严密的规则，建立起可靠的信任关系，并且深度嵌入数字信任体系。究其实质，是通过算法、规则和生态的深度融合，将传统社会信任关系从物理世界迁移到数字世界，把契约信任中对条款约定的遵守、技术信任中对技术稳定性的依赖进行重新整合，从而催生出电子签名数字信任这一全新模式。

电子签名数字信任模式的形成与新一代信息技术体系紧密相关，其中代表性的技术有三类：一是身份认证技术，最具代表性的是区块链，区块链的分布式账本和不可篡改特性，实现电子签名的全生命周期存证，打破了传统中心化CA机构的垄断地位，催生出去中心化的信任架构，构建起“技术自证”的新型信任关系。二是云计算技术，以“软件即服务”（Software as a Service, SaaS）解决方案的成熟为契机，云端电子签名平台迅速崛起，极大地提升了电子签名的普及率。三是人工智能技术，推进电子签名安全保障从“被动防御”转向人–机协作的“主动进化”，大大增强了电子签名的技术可信任度。在此背景下，逐渐形成了以电子签名为核心、多技术深度融合、制度治理支撑的社会–技术系统。随着系统不断巩固和加强，人们对电子签名的信任也不再只是依赖具体的个人或机构，而是将信任嵌入到社会技术–系统本身。

2020年疫情危机，电子签名从可选择的技术工具，转变为刚需的数字基础技术。根据36氪研究院的统计，2020年电子签名签署次数已突破500亿大关，较上年实现了317.51%的增长。[7] 置身于如此庞大且极具潜力的技术市场与广阔的应用前景之中，作为社会–技术系统存在的电子签名，离不开社会信任模式的支撑。电子签名的数字信任构建，标志着电子签名社会信任模式正在推进从单一的制度与技术保障，向多元融合“综合生态”的升级跃迁，目的在于打造一个全方位、多层次、整体性的数字信任网络。在这个网络中，技术、制度、市场、用户以及认证机构等行动主体相互交织、相互促进，为电子签名塑造一个契合数字文明需求的数字信任模式。

综上可见，电子签名契约信任、技术信任到数字信任这三种模式之间并非简单替换，彼此之间是相互加强、协力支撑的。电子签名的安全性和有效性取决于技术基础设施的稳健性，因此电子签名的契约信任依赖于技术信任的保障和支撑。技术信任是数字信任的关键组成部分，安全可靠的技术平台是社会对整个数字系统产生广泛信任的前提条件。在此基础上，数字信任提供了电子签名契约信任和技术信任运作的整体背景，塑造了用户对数字领域中值得信任行为的期望和监管标准。由此，可以认为在电子签名的演进历程中，电子签名技术与社会系统的深度交互特性，要求“契约信任–技术信任–数字信任”三者互补共进，进而形成一种“三位一体”的电子签名信任模式。这种“三位一体”的信任模式，不仅实现了技术应用与信任关系在数字场景中的有机适配，更通过不同应用场域的实践验证，持续强化电子签名技术的社会公信力基础，为电子签名在全社会范围内可信任性的实质提升，提供了可靠的模式支撑。

二、电子签名“三位一体”社会信任模式的风险挑战

1. 契约信任的悄然消解：技术与制度迟滞间的“撕裂”

（1）跨境法律不一致性。全球化的电子商务和数字交易要求电子签名要能够在不同的国别或地区司法管辖区内得到法律上的承认和执行。然而，全球各国对电子签名的法律处理方式均有不同程度的差异，部分司法辖区对电子签名在不同类型交易和相关活动中的技术标准、合规和认证流程有特殊要求。根据立法对电子签名技术是持放任还是管制的态度，可将各国的电子签名立法分为技术特定化、技术中立化以及技术折衷化三种技术方案。[8] 我国

的《电子签名法》属于折衷化方案，“采用‘功能等同主义’而非‘技术特定主义’”，[9]即不特定依赖于某一种技术实现电子签名。这种差异化的法律现状，可能会造成电子签名跨境使用的认可度和实际效力受到质疑，增加企业合规难度和跨境交易的风险复杂度。此外，不一致的法律框架还可能滋生跨境交易中的灰色地带。这种法律上的“模糊”不仅给交易双方带来了不确定性，也为不法分子提供了可乘之机，增加了跨境欺诈和违规行为的风险概率。

（2）电子签名证据链存在适用性断层。当前电子签名技术的司法应用正面临“技术超前、制度滞后”的结构性矛盾，这一矛盾集中体现在证据规则的适配性断层。从证据规则体系看，现行司法机制仍沿袭纸质文件时代的举证逻辑，在电子签名场景中机械套用“谁主张谁举证”原则，实质上形成了举证责任倒置问题。当用户需证明电子合同签署真实性时，往往因缺乏专业取证能力难以独立获取包含哈希值、时间戳、私钥操作日志在内的完整证据链，而现行《电子签名法》尚未明确云服务平台、CA认证机构等市场主体的证据保全义务，导致关键证据要素分散于不同技术主体形成证据链“孤岛”。更深层次的制度困境在于技术认证与司法鉴定的衔接断裂。CA认证机构缺乏司法鉴定资质，其出具的技术认证文件常需二次司法鉴定方可采信。导普遍存在的“二次鉴定”现象，不仅增加诉讼成本，还可能造成电子证据时效性折损，进一步导加剧事实认定困难。

2. 技术信任的瓦解危机：创新变革下的剧烈动荡与重塑

（1）密钥管理的脆弱性。私钥是公钥基础设施（Public Key Infrastructure, PKI）体系中最为敏感的核心组成，其安全性直接决定整个认证体系的可靠性。从技术实现层面看，签名者运用私钥对哈希后的数据进行签名操作，从而生成可以验证数据完整性及其来源真实性的电子签名。如果私钥泄露，攻击者可以冒充合法用户进行通信，或者伪造电子签名，进而破坏通信的完整性、身份验证和不可否认性。私钥泄露的风险来自多种因素，例如内部人员的恶意泄密、外部黑客的网络钓鱼攻击以及系统配置不当等。特别值得注意的是，在云计算和物联网环境下的分布式密钥管理场景中，密钥分发、轮换和撤销机制的复杂性指数级扩增，这显著放大了密钥泄露的潜在风险。攻击者可能利用通用签名伪造、增量保存、签名包装、中间人攻击、社会工程等手段窃取和篡改私钥。这些攻击手段不仅可能导致私钥的泄露，还可能引发更广泛的安全问题，如大范围的恶意软件传播、经济欺诈甚至网络战争。

（2）加密算法的安全性。传统电子签名的安全性依赖分解大质数或解决离散对数问题的难度。但这道安全屏障正在经历前所未有的考验，特别是量子计算机理论上可以逆向推演出数字密钥的生成规律，计算效率远超经典计算机，使得目前广泛使用的加密技术在量子计算面前变得十分脆弱。当运算能力突破某个临界点时，攻击者仅凭公开信息就能破解出核心密钥，意味着电子签名的唯一性认证将形同虚设。届时，既往习以为常的安全认证体系可能面临系统性崩塌，各类敏感信息的保护屏障将出现致命缺口。更棘手的是安全体系的升级换代绝非易事。从现行系统过渡到抗量子加密标准，既要保证业务连续性，又要防范升级过程中的衔接漏洞。这种新旧交替的“阵痛期”，往往也是安全防护最薄弱的危险期，稍有不慎就可能触发“多米诺骨牌”式的安全危机。

（3）CA认证机构职能错位。当前CA机构主要职能是对（签名用）私钥持有人进行认证并保证私钥发放过程的安全可信。私钥的实际应用则由平台方（应用方）主导，CA机构对私钥使用（签署）过程完全缺乏监管能力，难以完整履行可靠性保障责任。在制度建设和监管流程上，CA机构仅控制私钥的生成与分发，但私钥使用时的哈希计算、文件对象加密等关键操作均由应用系统自行实现，CA既无法验证签名对象与文件内容的一致性，也无法追溯私钥在具体业务场景中的实际调用逻辑。此外，CA机构技术保障能力不足，证据保全机制建设滞后，导致其无法对电子签名全流程提供有效存证支持。而市场用户的愿景是希望有

机构对电子签名全过程的可靠性进行保障，导致CA认证机构能够发挥的作用与社会公众的期望出现错位，仅能以部分环节的保障承担全流程安全责任，实际上是将《电子签名法》的实施置于风险之中。

3. 数字信任的迷惘不清：虚拟“迷雾”中的徘徊与踯躅

（1）数字鸿沟与机会不均。电子签名的普及应用在重构社会、商业流程的同时，也暴露出显见的技术包容性悖论。其技术实现高度依赖智能终端设备与网络基础设施的支撑，并要求使用者具备基础的数字素养与操作能力。在客观上构建起了一道隐性的准入壁垒。电子签名技术的复杂性、交互方式的多样性以及认证过程的繁琐限制，可能会使一些社会群体在使用电子签名时面临困难。尤其是农村留守群体、城市银发族群以及数字原住民之外的过渡型用户，在参与电子交易和签署电子合同时，可能会面临系统性的排斥风险。这种排斥不仅表现在技术操作层面的显性障碍，更延伸至数字权利获取的深层危机，即当电子签名成为获取公共服务、参与经济活动的基础要件时，技术弱势群体实质上被剥夺了平等参与数字社会生活的“入场券”。这种技术性社会排斥的持续发酵，不仅加剧了既有社会资源分配的整体性失衡，在技术正义层面引发深层伦理拷问。

（2）个人隐私保护问题。在电子签名的过程中，大量涉及个人身份和财务相关信息的采集、处理、存储与传输，这使得数据隐私和安全成为不容忽视的关键问题。在数字环境下，数据泄露和未经授权的访问是首要的安全隐忧。恶意攻击者可能通过各种手段入侵电子签名系统，窃取用户的敏感信息，从而对个人隐私和财务安全构成重大威胁。此外，电子签名平台本身在运营过程中也必须高度重视用户信息的安全。如果平台未能妥善保护用户数据，不仅会严重损害用户的权益，还会破坏公众对电子签名技术的信任。一旦信任基础动摇，电子签名技术的广泛应用将面临巨大的挑战和阻力。在签署合同或协议时，信息的传输过程同样充斥着多种风险问题。如果安全措施不到位，用户的敏感信息可能在传输过程中被第三方截获或篡改，导致隐私暴露、身份盗窃等严重后果。这不仅给个人带来不可挽回的损失，还可能对平台企业的声誉和法律责任产生直接影响。

（3）过度依赖与意义消解。传统签名通常需要手写或通过正式的印章进行，具有独特的个性化特征。在未来的深度数字化社会中，电子签名虽然提高了效率和便捷度，但也使得签名行为本身变得更加程序化和机械化，签名行为的象征意义和其承载的严肃性便不可避免地被削弱。人们可能在不自觉中忽略了签名所承载的法律责任和后果，对签名的重视程度下降。特别是对于那些缺乏技术背景的签名者而言，理解电子签名的技术原理、不同等级的签名类型以及其法律效力，往往是一个困难且令人困惑的过程。这种认知和素养的欠缺可能导致他们低估或误解电子签名的严肃性和重要性，在没有完全理解或仔细审查合同内容的情况下，快速作出签名决策，导致不负责任的签名行为，造成电子签名技术的滥用和误用，对电子签名技术的可信任性、数字经济的健康发展和社会的稳定产生严重的负面影响。

三、提升电子签名社会可信任度的优化策略

1. 创设联合监管中心，保障“三位一体”的体制机制支撑

电子签名技术作为数字经济时代的关键基础性技术，其监管效能不仅关乎数字政务转型与跨境贸易安全，更深刻影响着社会数字化转型进程的可持续性。针对当前电子签名监管领域存在的多头管理、标准分散、跨境互认不足等系统性挑战，亟需构建一个统筹协调、动态响应、内外联动的监管中枢机构。

第一，建议相关政府职能部门，成立联合监管中心，并附设专家委员会，负责制定出一套统一、规范的电子签名监管标准与操作流程，包括对CA、数字证书注册审批机构（Registration Authority, RA）等第三方电子签名服务商的严格资质审核与常态化监督，确保

其服务符合法律法规要求，并涵盖了对未来电子签名技术应用的全面指导与规范。

第二，联合监管中心应设立专门的科技情报机构，实时跟踪国内外电子签名领域的案件动态与学界研究成果，及时发现并评估潜在的安全风险与技术漏洞。以官方的权威名义，建立高效的风险预警机制，一旦发现问题和漏洞能够迅速向相关电子签名服务商及使用方发布预警通知，指导其采取有效措施进行防范与应对。

第三，联合监管中心可以与其他国家或地区的电子签名监管机构建立合作关系，通过签订互认协议等方式实现电子签名的跨境互认。在互认协议框架下对于希望进入我国市场的海外电子签名服务商，进行资质审核、技术评估与合规性检验，确保其符合互认协议的要求和标准。

2. 强化契约信任：夯实电子签名的制度基石

为实现电子签名从技术可行性向制度公信力的实质性跨越，克服纵深应用场景中制度供给滞后与技术创新加速的“异步空转”问题。亟需构建具有国际兼容性、行业适配性和技术前瞻性的制度框架体系，为数字时代的契约文明奠定法治基石。

第一，通过加强与国际组织、标准化机构和各国政府的深入合作，推动建立全球范围内的电子签名规则体系融合衔接，确保电子签名在国际贸易、跨境金融、电子商务等场景中的法律效力得以互认。与此同时，企业应当加强与全球电子签名服务商的合作机制建设，推动国际市场对中国电子签名技术和服务的信任和接受。

第二，随着技术的快速发展、应用场景的多样化和受众群体的多元化，应根据我国实际情况，针对不同行业、不同业务场景中的电子签名需求，明确其适用范围、使用规范和监管要求，根据金融、医疗、政务等领域的特殊要求，进一步细化电子签名的技术标准和法律效力条款。

第三，加强对国外先进经验的学习和吸收，借鉴其他国家和地区在法律法规方面的成功经验，结合自身发展实际，制定更加细化、可操作的法律规定。此外，立法过程中应充分考虑技术发展趋势，灵活调整相关法规，预见和应对未来可能出现的新技术和新应用场景，从而提升电子签名法律法规的供给弹性。

3. 优化技术信任：以创新驱动提升信任保障

面对全球数字安全需求升级的新形势、新要求和新挑战，亟需通过创新驱动重塑信任保障机制。这不仅关乎电子签名行业的战略主动权，更是筑牢数字中国安全基座的关键。需要以体系化的创新布局完善技术体系，通过产学研深度融合构建新一代技术“护城河”，加快实现可信技术供给与市场需求升级的同频共振。

第一，以密码科学技术全国重点实验室为核心，组建政产学研用协同创新联合体，共同研发新型电子签名技术与解决方案，提前布局下一代密码学技术，成立联合创新研究院/中心/产业实验室，推动区块链、人工智能、量子通讯等先进技术在电子签名产品的创新应用，抢占技术创新与市场制高点。

第二，建立电子签名技术创新激励机制，政府、行业协会以及企业可以设立专项基金或奖励计划，对在电子签名技术研发、应用推广以及便民服务等方面做出突出贡献的单位和个人给予表彰和奖励，包括资金支持、政策倾斜、税收见面和补贴等多样化形式。

第三，加强技术标准的制定与推广，可以避免各类电子签名技术和服务的碎片化，确保电子签名技术的互操作性与一致性，巩固和完善电子签名技术社会公信力的制度支撑。与此同时，政府和企业也应共同推动这些标准的实施与推广，确保电子签名技术的安全性、兼容性和扩展性得到充分保障，从而为行业的可持续发展奠定坚实基础。

4. 重塑数字信任：数字情景中探寻前行之路

随着数字化转型逐步迈入“深水区”，数字信任已从技术保障机制升维为新型社会治理命题。这其中，数字信任是数字生态良性发展的基石，面对数字化转型浪潮，需以系统性思维重构信任机制。通过政企协同、信用治理与认知革新三轮驱动，方能筑牢数字社会运行底座。

第一，应积极推动电子签名服务商与政府、银行、法律服务等机构的深度合作，形成“技

术标准共构–场景数据互通–治理规则互认”的链式化合反应，帮助电子签名服务商可以更好地融入不同业务场景和多样化的服务，鼓励公共部门与私营企业共同推动电子签名的普及应用，提升技术应用的可信度和覆盖面。

第二，建立信用评价体系和动态信用图谱，对服务商的技术能力、安全性保障、用户满意度等方面进行动态评估。通过定期审核、用户反馈、第三方认证等方式对电子签名服务商的信用状况进行公开披露，加快形成“数据画像–信用评级–市场择优”的良性循环，倒逼行业服务段位升级。

第三，加强电子签名科学普及，借助官方媒体宣传及教育培训，向公众普及电子签名知识。同时培训相关从业者。针对中老年及技术知识欠缺群体，开展社区科技服务，降低使用门槛。加强对青少年教育引导，将电子签名与密码学知识融入通识教育体系，奠定良好社会文化基础，为数字生态进化注入持久动能。

［参 考 文 献］

[1]Gupta, A., Tung, Y. A., Marsden, J. R. 'Digital Signature: Use and Modification to Achieve Success in Next Generational E-Business Processes'[J]. *Information & Management*, 2004, 41(5): 561–575.

[2] 罗文华. 规则与共识: 从电子签名到区块链 [J]. 中国政法大学学报, 2019, 13（2）: 48–59; 206.

[3]Diffie, W., Hellman, M. E. 'New Directions in Cryptography'[J]. *IEEE Transactions on Information Theory*, 1976, 22(6): 644–654.

[4]Rivest, R. L., Shamir, A., Adleman, L. 'A Method for Obtaining Digital Signatures and Public-Key Cryptosystems'[J]. *Communications of the ACM*, 1978, 21(2): 120–126.

[5] 杨昊. 区块链: 从密码朋克到人类命运共同体 [J]. 国际论坛, 2021, 23（2）: 53–71; 157–158.

[6] 刘晗. 密码朋克与个人隐私的未来 [J]. 读书, 2023, 51（10）: 95–103.

[7]36氪研究院. 2021年中国电子签名行业研究报告 [R]. 36氪研究院, 2021.

[8] 蔡虹、夏先华. 电子签名证据真实性的多维检视: 保真、鉴真与证明 [J]. 湖南社会科学, 2019, 32（5）: 61–70.

[9] 邢爱芬、付姝菊. 中国电子签名立法与实践问题研究 [J]. 科技与法律（中英文）, 2022, 32（3）: 14–23.

［责任编辑　李斌］