金融场景电子签名应用趋势及其法律效力认定的探讨

文丨 王红叶 钟宇 黄莉群 赵蝶

在推动数字金融高质量发展的进程中，电子签名作为金融数字化转型的信任抓手，其应用场景逐步从零售信贷、融资租赁、电子保单、网上证券向供应链金融、智能投顾、跨境贸易等多元领域延伸。社会各界对电子签名的认知度持续提升，与之相伴的是相关司法纠纷案件亦在同步增多。裁判文书网检索数据显示，涉及“电子签名或数字签名”的合同纠纷判决累计 72371 件，其中金融借款合同纠纷 59749 件，占比高达 82.6%，“签名非本人”“证据非原件”等成为高频抗辩理由。基于主流数字证书技术的电子签名，在司法纠纷案件中的“证明力”日益成为金融机构关注的焦点。

电子签名证据被司法采信的核心要点

合规电子签名的认定依据

在金融场景电子签名的应用中，合规电子签名的认定需以明确的法律法规为核心依据。当前《中华人民共和国电子签名法》（以下简称《电子签名法》）是界定电子签名合法性、可靠性及法律效力的核心法律文件。《电子签名法》第十四条明确规定：“可靠的电子签名与手写签名或者盖章具有同等的法律效力。”这一规定打破了“书面中心主义”的传统桎梏，为电子签名在金融业务中的广泛应用提供了法律基础。

涉诉案件中的司法审判思路

第一个维度是合法性审查。在这一维度的审查中，重点涵盖电子签名适用范围的界定、当事人是否具备真实签署意愿的认定，以及金融机构在电子签名使用过程中应履行的告知、提示等义务的落实情况，上述内容共同构成了合法性审查的核心框架，旨在从法律适用、意思表示、义务履行等层面，判断电子签名的合法属性。

第二个维度是原件判断。该维度的核心审查内容包括电子签名对应的“原件”认定标准、提供电子签名服务的第三方平台是否具备合法资质，以及电子签名相关证据链是否完整且无断裂。法院通过明确“原件”的电子形式认定规则、核查第三方平台的合规资质、核验证据链的连贯性等方式，确保电子签名所对应的证据能够达到与传统纸质原件相当的证明效力。

第三个维度是可靠性审查。该维度的审查主要聚焦于电子签名的三大关键属性，即专有性、控制性及防篡改性。专有性指电子签名需与签名人形成唯一对应关系，控制性指签名人能够独立控制签名行为，防篡改性指电子签名生成后与之关联的数据内容不可被随意篡改。这三个相互支撑、缺一不可的属性共同构成电子签名可靠性的核心评判指标，也是法院判断电子签名是否具备可靠证明力的重要依据。

电子认证发展新阶段下电子签名合规性探讨

电子认证发展阶段与新需求

1．电子认证发展阶段

在电子认证服务的演进历程中，其技术架构与应用范式经历了三轮关键性跃迁。自 1.0 时代以 USBKey 等硬件载体为核心的数字证书体系着力破解身份认证环节的安全防御与操作便捷性矛盾，进而至 2.0 时代电子签名技术跃升为数字化转型的核心驱动力，全面推动金融、政务等领域的业务文档无纸化处理、服务渠道在线化迁移及交互方式移动化变革，最终进至 3.0 时代。该时代以分布式数字身份认证、自主主权身份管理、区块链存证验证以及后量子密码算法等数字信任技术群为支撑，构建起贯穿业务全周期、覆盖场景全维度、渗透流程全环节的可信交互生态系统，为金融行业数字化转型提供更具弹性与韧性的认证基础设施。

2．3.0 时代金融电子签名应用新需求

（1）场景分化带来的电子签名差异化应用

现行法律框架对金融领域多样化场景缺乏分级分类规范。同时，区块链智能合约签名、后量子密码技术等新兴技术的应用，导致技术创新与法律适配出现失衡，迫切需要构建覆盖金融全场景的分级认证制度及动态更新的电子签名司法解释体系。从业务风险维度分析，高风险领域的电子签名要求已形成普遍共识，对于信贷合同签署、理财协议订立、跨境支付等直接涉及用户大额资金安全、权利义务核心变更的业务，均明确要求采用符合《电子签名法》规定的可靠电子签名，以保障业务的法律效力和风险防控能力。然而，在中低频、低风险业务场景中，争议却持续存在，例如账户信息变更中联系电话或地址的修改、常规客服工单处理中业务咨询记录的确认，关于这些操作是否需要强制使用可靠电子签名，目前尚无统一标准。实践中一旦发生劳动纠纷或内部责任争议，此类电子签名的法律效力仍可能面临司法质疑。

（2）业务移动化重新定义密钥载体形态

在电子认证 3.0 时代，传统的物理介质 UKey 向移动端的可信执行环境（TEE）与安全元件（SE）加速演进。业务移动化趋势正深刻重塑密钥存储容器的形态，亦为云签名、一次性签名、协同签名等新型签名模式的应用提供了条件，同时引发了对其合规性讨论。首先，云签名的核心争议在于“密钥存于云端，如何证明仅用户能够控制”，鉴于云端由平台进行管理，如何确保符合《电子签名法》中“签名制作数据仅由签名人控制”的规定，避免平台越权调用或密钥泄露情况的发生。其次，一次性签名的争议主要集中在“密钥使用一次即作废，若后续需要验证签名效力，如何证明当时为本人签署”。因此，必须保证每次密钥具有唯一性且使用后即销毁，同时留存签名时间、操作记录等相关痕迹，以满足“签署后改动可发现”的要求，防止有人利用旧密钥冒充签名。最后，协同签名的争议则是“多人签字时，如何确定每个人均为自愿签署，避免出现‘他人代签’或‘签字顺序混乱导致责任界定不清’的情况”。

电子认证 3.0 时代电子签名核心挑战探讨

电子签名 3.0 时代的核心特征，体现为技术架构从“单一物理介质存储”向“移动端 TEE/SE 与云端分布式存储”转型，场景应用从简单线上签署向多主体、跨领域复杂业务延伸。这一变革与新规对合规性、安全性的更高要求叠加，使得核心挑战集中于身份核验、密钥控制、存证链构建三大维度，且各挑战均呈现“技术特性与合规标准不匹配”的内在矛盾：身份核验责任重构的挑战根源在于，3.0 时代核验模式从“单方主导”转向“多方协同”，与新规“责任可追溯”要求存在逻辑断层。传统模式下，金融机构作为单一核验主体，责任边界清晰。而 3.0 时代，身份核验需用户、技术提供平台、第三方存证机构共同参与，形成“用户提交信息 - 平台技术核验 - 机构存证结果”的协同链条。但新规仅明确了“责任需可追溯”的原则性要求，未界定不同参与方在“核验规则设计、技术风险防控、结果存证验证”等环节的责任分配标准，导致“技术缺陷引发的核验失误”“跨主体数据流转中的责任衔接”等问题缺乏统一判定逻辑，进而造成责任边界模糊，影响合规体系的系统性落地。

密钥控制合规界定的挑战，本质是 3.0 时代密钥存储形态的“间接化”“封闭化”，与新规“签名制作数据仅由签名人控制”要求的适配冲突。3.0 时代，云端存储通过 HSM 模块实现密钥集中管理、移动端 SE 通过硬件隔离实现密钥封闭运行，两种模式均使密钥脱离用户直接掌控，用户仅能通过身份验证间接调用密钥，无法直接接触或管理密钥本身。这种技术层面的“控制权间接性”，与《电子签名法》中“控制权专属”的法律界定形成偏差：“间接调用”是否等同于“实质控制”？“技术封闭管理”是否构成“控制权让渡”？当前新规未针对新型存储形态细化控制权认定标准，也未明确“密钥拆分存储”等技术方案的合规性，导致实践中合规界定缺乏统一依据，陷入理论与技术脱节的困境。

存证证据链完整性的挑战，核心是 3.0 时代业务场景的“碎片化”“跨平台化”，与新规“全流程可追溯、长期存储”要求的实践落差。3.0 时代电子签名需适配供应链金融、跨境支付等多场景，证据链需覆盖“业务授权 - 身份核验 - 签名操作 - 结果归档”全环节，且涉及多平台数据互通。但新规未明确证据链的核心构成要素与数据标准，既未界定“业务前置材料（如授权文件）是否需纳入存证”，也未统一跨平台数据的格式与验证规则，导致实践中易出现“关键环节数据缺失”“跨平台数据衔接断裂”等问题。

电子签名应用发展趋势与合规性探讨

场景化应用：分级分类与司法认定统一化

针对不同风险等级业务场景下的标准混乱问题，未来的核心发展趋势将围绕“分级分类法治化、场景适配精准化、司法认定统一化”展开。首先，将推动电子签名应用范围的分级分类规则落实到法律与行业规范层面，可借鉴欧盟《电子身份认证与信任服务条例》（eIDAS）中“根据业务风险等级匹配不同安全强度签名要求”的思路，在国内立法或司法解释中明确划分高、中、低风险业务边界：对信贷合同、跨境支付等已形成共识的高风险场景，固化可靠电子签名的强制适用标准。对账户信息简单变更、常规客服记录确认等低风险场景，明确非强制性可靠电子签名的适用空间，允许采用符合基础安全要求的轻量化签名方式，同时界定此类签名的法律效力边界。其次，将建立场景化的动态调整机制，结合金融业务创新节奏，定期更新风险等级目录与对应签名标准，避免因规则滞后导致应用范围模糊。最后，将通过发布典型司法案例、出台专项指导意见等方式，统一法院对“内部业务电子签名可靠标准”的认定尺度，消除司法层面的不确定性，反向推动电子签名应用范围界定的清晰化，既保障高风险业务的合规安全，也为低风险业务的效率提升释放空间。

合规与安全效率平衡：体系化升级与技术创新

电子认证 3.0 时代，未来电子签名将围绕三大方向优化，以实现技术合规与安全效率平衡。一是，身份核验体系升级为“CA 自主核验 + 金融机构协同”模式，CA 对接权威平台完成客户基础身份认证并生成数字证书，金融机构结合业务风险补充场景化核验，同时建立核验结果互认机制，解决跨境追溯难与多主体责任模糊问题；二是，密钥控制模式转向“分级 + 技术创新”，按风险等级差异化设计存储与授权规则，低风险业务简化操作、高风险业务强化安全，引入密钥拆分

（下转第 96 页）