面向真实性的版式电子文件签审流程研究

张泽升　易雨洁
（广州市微柏软件股份有限公司，广州 510510）

【摘要】文章剖析了实践工作中“在线编辑器生成文件 + 事后批量签名”“审签分离 + 后台代签”两大典型电子文件签审流程违规模式，分析了具体风险，构建了“建设合规签审流程、落实合规签审功能需求、明确合规签审管理规定、加强行业监管与培训”四位一体的治理体系，以期为保障电子文件真实性提供可落地的理论参考与实践路径。

【关键词】电子文件；电子档案；真实性；签审流程；电子签名

【作者简介】张泽升，广州市微柏软件股份有限公司电子档案事业部总经理，副研究馆员，信息系统项目管理师，邮箱：1194800632@qq.com，研究方向为电子文件归档、电子档案管理；易雨洁，广州市微柏软件股份有限公司解决方案工程师，研究方向为工程电子档案管理。

1 引言

数字转型浪潮下，电子档案凭借存储便捷、流转高效、易于共享等优势，正逐步替代传统载体档案。《中华人民共和国档案法》（以下简称《档案法》）明确了“电子档案与传统载体档案具有同等效力”“确保电子档案的真实性、完整性、可用性和安全性”[1]。其中，电子档案的真实性，一般通过对固化信息是否有效、元数据项是否规范等方面来进行验证[2]。固化信息主要包括数字摘要、SM3、电子签名、时间戳等技术措施。

《中华人民共和国电子签名法》（以下简称《电子签名法》）明确提出“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”，同时明确可靠电子签名四要件，即签名制作数据归签名人专有，签署时仅由签名人控制，签名及内容改动可被查验，文件内容与形式改动可被查验[3]。《电子印章管理办法》（国办发〔2025〕33 号）第二十一条确立了“谁所有、谁控制、谁签章、谁负责”的使用管理原则，第二十二条明确“电子签章过程信息应当被记录并保存，实现电子签章行为可追溯、可定责”[4]。

《电子档案管理办法》（国家档案局令 第 22 号）提出“电子文件归档格式应当具备开放、不绑定软硬件、显示一致性、可转换、易于利用等特性，并能够支持向长期保存格式转换”[5]。《版式电子文件长期保存格式需求》（DA/T 47-2009）[6] 和《电子文件归档与电子档案管理规范》（GB/T 18894-2016）[7]，也提出了类似的要求。《电子档案单套管理一般要求》（DA/T 92-2022）要求，电子文件审核、签发、签章等关键节点必须完整留存修改痕迹与全流程元数据[8]。

依据电子档案管理与电子签名相关规定和要求，电子文件归档与长期保存工作中主要推荐使用的文件格式是 PDF/A 和 OFD/A。PDF/A 和 OFD/A 作为静态内容能满足档案管理与电子签名双重要求的格式，通过强制嵌入字体、禁止外部依赖、固

化版面结构，确保了电子档案在未来数十年，甚至更长时间的技术迭代后，仍可准确还原。

然而，在面向归档的版式电子文件在快速推广应用过程中，电子签审的违规乱象已呈蔓延之势。例如“在线编辑器生成文件 + 事后批量签名”“审签分离 + 后台代签”等违规做法普遍存在，这些做法表面上完成了电子签名，实质上却破坏了电子文件的真实性。

本文剖析了上述违规签审现象及其风险，并提出了面向真实性的版式电子文件违规签审流程治理路径，以期为保障电子文件真实性、实现电子档案规范化推广提供可落地的理论参考与实践路径。

2 版式电子文件签审流程的典型违规现象分析

2.1 两大典型违规流程剖析

2.1.1 模式一：在线编辑器生成 + 事后批量签名

该模式下，业务人员使用支持多人协作的通用在线编辑器生成普通 PDF 文件，文件保留编辑接口与外部依赖，未通过版式锁定与权限控制机制固化文件内容。业务系统仅留存简易审批记录，未嵌入标准归档元数据。审批流程全部办结后，系统后台归集所有个人 CA 私钥，跳过身份核验，一键批量完成所有签名，将违规事后批量签名后的普通版式文件直接归档。

2.1.2 模式二：审签分离 + 后台代签

该模式刻意借用“审签分离”概念混淆合规边界，审批人在业务系统中完成全流程线上审批，系统留存审批表单，但审批记录与文件本体相互分离，未实现元数据绑定。更为关键的是，签名环节绕过本人授权，由系统后台统一调取责任人的个人私钥，自动批量完成各方签名，所有签章时间精确到同一秒，操作日志批量生成，无独立履职记录，难以追溯责任人，却对外宣称“审签分离合规文件”。

以上两种模式在《电子签名法》第十三条规定的“可靠的电子签名”四要件方面均存在违规行为：第一，数字证书私钥由后台统一控制，并非签名人本人专有，违反“专有性”要求；第二，签名人未在签署时实际控制私钥，签名行为由系统后台代为完成，违反“控制性”要求；第三，批量生成的标准化签名数据可被复制替换，签名本身被改动后难以察觉，违反“签名防篡改”要求；第四，文件生成、业务审批与电子签名在时序上相互脱节，文件在签名前可能被系统后台替换、增删或格式重排，而事后补签无法对签署时的文件状态进行即时哈希固化与密码学绑定，导致文件内容与形式发生改动后无法通过签名进行独立查验，违反“内容防篡改”要求。

2.2 违规签审流程风险剖析

以上两类违规签审模式在实际运行中将引发以下三重连锁风险。

2.2.1 法律效力风险

事后批量签名与后台代签两种违规模式本质上都是用系统自动化代替签名人的控制与确认。然而，在追求操作效率的过程中省略了关键控制环节，不仅牺牲了法律行为的严肃性，也削弱了元数据的准确性和完整性 [9]。此类电子文件无法满足司法审查中的真实性、关联性与合法性检验要求，更会导致大批文件集体失效的链式污染风险。同时，后台统一归集个人私钥的操作，违背了《电子印章管理办法》（国办发〔2025〕33 号）第二十一条“谁所有、谁控制，谁签章、谁负责”的原则，存在行政追责风险。

2.2.2 档案合规风险

违规模式生成的电子文件在移交接收环节存在真实性问题，无法满足《档案法》关于电子档案“来源可靠、程序规范、要素合规”的要求，难以“以电子形式作为凭证使用”。同时，这类电子文件归档后形成的电子档案也无法满足进场交易所要求的“归档完整性、内容合规性、保管安全性”质量标准 [10]。此类违规生成、无法交易的电子档案不仅将导致业务资质审查受阻，更可能面临经济损失、行政处罚甚至刑事责任。

2.2.3 技术安全风险

文件属性层面，违规签审模式下生成的电子文件采用非归档格式，面临内容可被篡改、元数据不完整等真实性问题，不能满足电子文件归档的基本要求。系统安全层面，事后批量签名工具和后台代签私钥库一旦被内部滥用或外部攻破，操作者即可利用集中控制的私钥批量伪造文件签名、冒用任意责任人账户进行虚假签署，且系统审计日志无法区分真实签署与后台代签行为。管理追责层面，两种违规签审模式将签名控制权让渡至系统后台，存在无法追溯、无人担责的管理漏洞，最终仍将由所在机构承担额外的财务与法律风险。

3 面向真实性的版式电子文件违规签审流程治理路径

3.1 建设合规签审流程

3.1.1 推荐使用一步一签模式

一步一签模式是指在电子文件生成的关键业务节点，由责任人通过其专有私钥实时施加电子签名，签名行为与审批行为同步完成，时间戳与文件内容

即时固化。该模式以“文件生成即锁定、审批即留痕、签署即固化”为技术原则，其标准操作流程如下。

首先，文件生成与版式锁定。审批流程在业务系统发起后，系统会自动生成符合归档要求的版式电子文件，并通过版式锁定与权限控制机制禁止二次编辑，确保文件内容从生成之时即处于封闭状态。其次，在线审阅与意见固化。负责人在线审阅后签署审核意见，作为业务元数据同步嵌入文件属性，与文件内容共同构成完整的审批记录，从而满足“签名人认可内容”这一法律前提。再次，身份核验与数字签名。签署意愿确认完毕后，签名人通过身份核验调用个人私钥；系统采用国密算法对电子文件完整内容计算哈希值（即数字摘要），签名人使用私钥对该摘要进行签名运算生成签名值，并将包含签名值、签名证书、时间戳的签名数据以增量更新方式追加嵌入版式文件，确保原文件结构不被破坏。最后，日志固化与责任锁定。签名动作一经完成，系统即时生成独立操作日志与可信时间戳，元数据在时序上保持高度统一。签名全过程由签名人独立操作，系统仅提供技术通道，不得进行后台干预，从而确保签署行为的专有性、控制性与责任链条的完整性与可溯源性。

3.1.2 有条件推荐规范审签分离模式

审签分离指业务审批与电子签名在操作环节上由不同主体或在不同系统中分步完成，但各自独立留痕。审签分离通常表现为：业务审批（审）→审批结论形成→电子签名（签）→归档。业务系统中，审批结论形成后，由责任人分时序、分账号、独立调用其个人私钥完成签名，生成独立的时间戳与签名日志（含审批人、审批意见、审批时间）。此模式下，审批元数据与签名元数据虽物理分离，但可通过统一编号建立关联映射，两者相互印证，仍具有真实性，属合规归档。

3.2 落实合规签审功能需求

依托合规 CA 机构签发的数字证书构建信任根基，在应用系统层面实现以下关键功能要求。

3.2.1 前置身份绑定

为实现签名人身份与数字证书的强绑定，需严格执行以下要求：一是数字证书申请须通过身份证件核验与人脸识别的双重实名认证，不得由管理员批量代为申请；二是系统不得提供在服务器端或软件库中生成并代管私钥的功能，系统管理员不应拥有直接调用用户私钥的接口权限；三是证书有效性未通过系统验证时不能进行签名；四是数字证书的发放、调取、更新、注销等操作须经签名人本人二次确认。

3.2.2 签署前意愿确认

文件一旦进入待审批签名流程，系统自动执行内容锁定并实时计算哈希值，任意改动均会重新生成新的文件版本。签名人通过身份校验，需完整预览文件后才能执行个人意愿确认操作，并实时完成。

3.2.3 签署时单次单签

签名过程只能在签名人控制的终端介质内完成，意愿表达与签名运算不可分割。即使是同一签名人连续签署多份文件，也必须先发起独立的意愿确认与私钥运算流程，系统不得提供任何形式的签名复用或批量套用功能。签名完成的同时，系统自动加盖时间戳，与签名值、哈希值一同打包固化，形成不可篡改的签名结果。

3.2.4 签署后校验固化

签名完成后，系统服务端自动对签名进行比对校验。若校验不通过，系统自动回退流程并反馈异常信息，相关文件不得进入后续审批环节或归档。若校验通过，系统会将文件本体与签名相关数据一同绑定固化，杜绝事后篡改风险。

3.2.5 明确审签模式边界

若业务场景确需采用“先审核、后签名”模式，必须确保审签分离操作规范。审核阶段在业务系统中留存完整独立的审批元数据，签名阶段由各责任人分时段、分账号独立签章，各签名时间戳互不重复。应将事后批量签名、违规审签分离等行为划定为技术红线，严格禁止。

3.3 明确合规签审管理规定

3.3.1 明确签署工作要求

档案主管部门独立，或者与行业主管部门联合，出台电子文件签署相关实施细则，明确归档 / 长期保存的电子文件格式必须为 PDF/A 或者 OFD/A，并采用一步一签或者合规的审签分离模式；明令禁止事后批量签名、后台代签、虚假审签分离等行为，划定不可逾越的行业红线，确保电子文件的真实性。

3.3.2 落实个人数字证书权属与管控责任

各单位须在文档管理制度体系中明确数字证书的权属关系与管控义务，证书及对应私钥归签名人本人专有，任何机构或个人未经授权不得归集、代管或调用。应通过常态化宣传强化全员认知，并区分责任情形：因签名人本人出借、泄露私钥导致的违规签名，由签名人承担主要责任；因系统后台代签、批量调用等未经授权操作导致的签名违规，由系统服务商承担主体责任。此外，系统服务商应定期对业务系统中的签名模块进行渗透测试和抽样比对，若发现疑似事后批量签名或后台代签等违规行

为，须立即上报并组织排查。

3.3.3 建立电子文件合规考核与追责制度

各单位应将电子文件合规情况纳入部门与个人的绩效考核指标，建立清晰透明的责任追究机制。对故意使用事后批量签名、后台代签等违规签审模式，致使电子文件失去真实性，影响审计或验收等情形，按规定追究相关人员的责任。

3.3.4 对接专项验收与司法要求

各单位，尤其是工程、政务等领域，在遵循文件档案管理相关法律法规与规章制度、维护电子文件“四性”的同时，应紧密对接司法审查领域“三性”要求，将相关管理与技术措施，如使用符合归档要求的版式文件、一步一签模式、元数据完整且时序统一等，确立为电子文件验收与移交的准入条件，在制度层面杜绝失去真实性的电子文件进入验收程序。

3.4 加强行业监管与培训

3.4.1 开展专项排查整治

由行业主管部门或者联合档案主管部门组织开展专项自查与检查，全面排查采用违规模式进行签审的单位或项目。将电子签名合规性纳入归档验收必查项；对不符合真实性要求的电子文件归档行为，下达整改通知书；对整改不到位的单位或者系统服务商，采取进一步的惩罚措施。对于已经采用违规签审模式、尚处于质保期与追责期内的重要档案，应重新发起合规流程，组织规范化补签，形成新的合规档案，并保留原文件的溯源证据。若通过违规签署模式产生的档案已过追责期，应建立专项管理台账，注明问题情况后单独存放，根据国家规定的档案鉴定与销毁程序另行处理。

3.4.2 提升相关人员素质

面向文件档案管理人员、业务经办人员及系统服务商开展分层培训：文件档案人员重点掌握“四性”检测技术，尤其是真实性检测，包括版式文件验证、数字签名验签、元数据审计等技术技能；业务人员重点强化一步一签操作规范与法律风险意识；系统服务商重点提示违规签署的风险与法律惩处。同时，鼓励档案工作人员考取档案数字化管理师等职业资格，破解档案专业人才数字素养不足的困境。

注释及参考文献

[1] 中华人民共和国档案法 [EB/OL].(2020-06-20)[2026-06-24].https://www.saac.gov.cn/daj/falv/202006/79ca4f151fde470c996bec0d50601505.shtml.

[2] 王大众 .《文书类电子档案检测一般要求》解读 [J]. 中国档案 ,2019(4):34-35.

[3] 中华人民共和国电子签名法 [EB/OL].(2019-04-23)[2026-06-24].https://flk.npc.gov.cn/detail?id=ff8080816f135f46016f2163e4261aa1&title= 中华人民共和国电子签名法 .

[4] 国务院办公厅关于印发《电子印章管理办法》的通知 [EB/OL].(2025-09-27)[2026-06-24].https://www.gov.cn/gongbao/2025/issue_12346/202510/content_7044732.html.

[5] 电子档案管理办法（国家档案局令 第 22 号）[EB/OL].(2024-11-01)[2026-06-24].https://www.gov.cn/gongbao/2024/issue_11746/202412/content_6991650.html.

[6] DA/T 47-2009 版式电子文件长期保存格式需求 [S].

[7] GB/T 18894-2016 电子文件归档与电子档案管理规范 [S].

[8] DA/T 92-2022 电子档案单套管理一般要求 [S].

[9] 张瑞华 , 郑毅 , 高大伟 . 电子档案中电子印章“去技术化”的法律问题及解决路径 [J]. 档案管理 ,2025(2):24-28+33.

[10] 郑州市公共资源交易中心 . 定西：全面开展工程类进场交易项目档案专项核查 [EB/OL].(2026-07-06)[2026-07-24].https://zzggzy.zhengzhou.gov.cn/xyzx/20260706/dee22d9f-f3b4-45f2-aa88-3d47db45e044.html.

Research on the Authenticity oriented Format Electronic Document Signing Process

ZHANG Zesheng, YI Yujie
(Guangzhou Weibai Software Co., Ltd., Guangzhou 510510)

Abstract: This article analyzes two typical violation modes of electronic document signing and approval processes in practical work, namely "online editor generated files+post batch signatures" and "separation of review and approval+backend proxy signatures". It analyzes specific risks and constructs a governance system that integrates "building compliance review and approval processes, implementing compliance review and approval function requirements, improving review and approval work management mechanisms, and strengthening industry supervision and training", in order to provide practical theoretical references and practical paths for ensuring the authenticity of electronic documents.

Keywords: Electronic files; Electronic archives; Authenticity; Sign off process; Electronic signature