ICS 35.020

CCS L77

T/ SIA

中 国 软 件 行 业 协 会 团 体 标 准

T/SIA066—2025

第三方服务电子档案真实性验证技术规范

Technical Specifications for Third-Party Service Electronic Records Authenticity Verification

2025-12-18 发布　　2025-12-18 实施

中 国 软 件 行 业 协 会 发 布

目　录

前 言

本文件按照GB/T 1.1-2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国软件行业协会提出并归口。

本文件起草单位：北京联合大学、国家开发投资集团有限公司、北京星震同源数字系统股份有限公司、北京联合信任技术服务有限公司（联合信任时间戳服务中心）、北京汉龙致远科技有限公司、清华大学第一附属医院、贵州省测绘资料档案馆。

本文件主要起草人：谢永宪、宋萍萍、赵伟东、张昌利、毕向阳、舒蓉、仇寿霞、郑昳、王思斯。

第三方服务电子档案真实性验证技术规范

1 范围

本规范旨在制定第三方服务电子档案真实性验证的技术规范，以维护和验证电子档案及其元数据的法律效力。本规范适用于第三方服务机构在提供电子档案相关服务过程中，对电子档案真实性验证的技术要求和操作管理。

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。

[1] GB/T 18894-2016 电子文件归档与电子档案管理规范

[2] DA/T 92-2022 电子档案单套制管理一般要求

[3] DA/T 93-2022 电子档案移交接收操作规程

[4] DA/T 97-2023 电子档案证据效力维护规范

[5] SF/T 0076-2020 电子数据存证技术规范

[6] SF/Z JD0402004-2018 电子文档真实性鉴定技术规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

电子数据 digital data

以电子手段生成、发送、接收或者储存的信息。

[来源：GB/T 25069-2010 信息安全技术 术语]

3.2

电子文件 electronic records

国家机构、社会组织或个人在履行其法定职责或处理事务过程中，通过计算机等电子设备形成、办理、传输和存储的数字格式的各种信息记录。电子文件由内容、结构、背景组成。

[来源：GB/T 18894-2016，3.1]

3.3

电子档案 electronic archives

具有凭证、查考和保存价值并归档保存的电子文件。

[来源：GB/T 18894-2016，3.2]

文中使用“电子数据”对情况较多。需要注意两者的区分。(增加了定义，见3.1）

3.4

电子档案单套管理 single set filing management of electronic records

电子档案单套管理 仅以电子形式归档电子文件和管理电子档案的方式。

[来源：DA/T92-2022，4.7]

3.5

电子档案真实性 authenticity of electronic records

电子档案的内容、逻辑结构和形成背景与形成时的原始状况相一致的性质。

[参考：GB/T 18894-2016，3.5]

3.6

电子档案真实性验证 verification of the authenticity of electronic records

对电子档案的形成和管理过程进行分析，判断其修改情况。

[参考：SF/Z JD0402004-2018，3.5]

3.7

第三方 Third Parties

独立于直接参与方之外的组织或个人，在特定的交易、协议或过程中起到中介或验证的作用。

3.8

第三方存证验证 Third-party Evidence Preservation and Verification

由独立于电子数据或信息提供方和接收方的权威机构或服务，对数据或信息的来源、内容、完整性和生成过程等进行存证和验证，提供一种独立且客观的确认，以增强数据或信息的真实性和可靠性。

3.9

哈希算法 Hash Algorithm

哈希算法是一种数学函数，它接收一个输入（或“消息”），然后通过一种确定性的过程，返回一个通常更短的、固定大小的数据集，称为“哈希值”或“哈希码”。哈希算法的主要特点包括：确定性、单向性、抗碰撞性。

3.10

可信时间戳 Trusted Time Stamp

能证明数据电文（电子文件）在一个时间点是已经存在的、完整的、未被篡改的且可验证的，具备法律效力的电子凭证。

[来源：GB/T 42971-2023 第三方电子合同服务平台信息安全技术要求，3.7]

3.11

数字签名 Digital signature

数字签名，又称公钥数字签名，是一种用于验证信息来源和完整性的安全技术。数字签名的原理主要基于非对称密钥加密和数字摘要技术。非对称密钥加密采用一对密钥，即公钥和私钥。公钥用于加密信息，私钥用于解密信息。数字签名过程中，发送者使用私钥对信息进行加密，生成数字签名。接收者使用发送者的公钥对数字签名进行解密，验证信息的真实性和完整性。

4 系统架构

文件生命周期可以历经业务系统、档案管理系统、长期保存系统三个系统。电子档案真实性保障系统与文件生命周期的三个系统相互关联。作为独立的监督者和证据保全者，电子档案真实性保障系统对文件流转的关键节点和操作进行存证，为整个过程提供安全、合规、可信的证据支持。

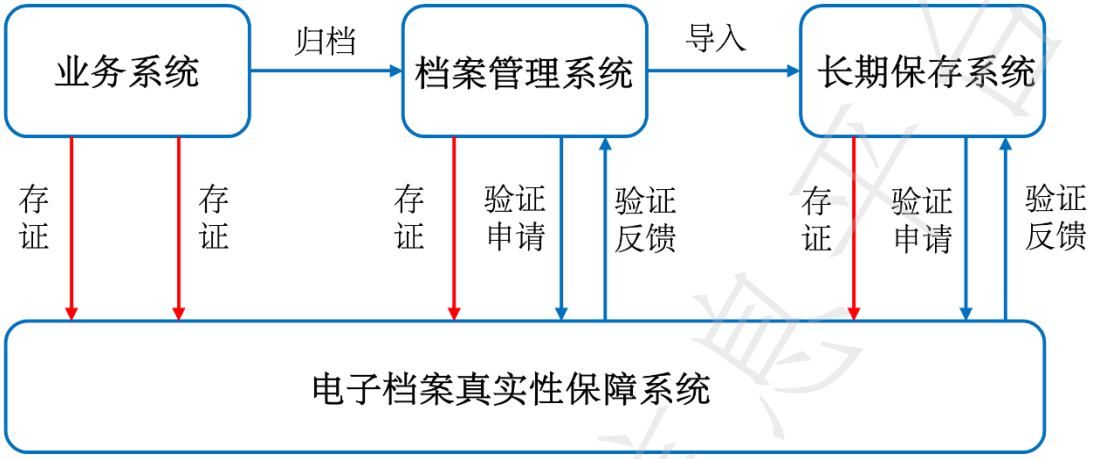

图1：电子文件全生命周期管理三系统与电子档案真实性保障系统的关系

4.1 业务系统

在业务系统，需对电子文件及其元数据进行存证信息收集。如图1所示，需要具备存证功能接口。

4.2 档案管理系统

需对档案管理全流程进行存证信息收集，涵盖归档与移交、存储与保管、格式转换、提供利用及销毁等关键过程。如图1所示，需要具备存证验证功能接口。

4.3 长期保存系统

长期保存系统作为电子档案的最终归口管理环境，需对各类介质保存的电子档案及其元数据进行存储与管理。如图1所示，需要具备存证验证功能接口。

4.4 电子档案真实性保障系统

电子档案真实性保障系统独立于业务系统、档案管理系统和长期保存系统，使用一系列技术手段来保障电子档案的真实性，并可对电子档案的真实性进行有效验证。

第三方提供单机、局域网、互联网三种环境，通过网站、应用程序和编程接口等形式提供电子数据存证验证服务。

适配不同的业务系统，电子档案真实性保障系统可一站式覆盖单机、局域网及互联网场景的存证验证需求。适配不同的档案管理系统，电子档案真实性保障系统需支持单机及局域网场景的存证验证需求。

表1：电子档案真实性保障系统与业务系统、档案管理系统的适配

验证环境	业务系统	档案管理系统
单机	√	√
局域网	√	√
互联网	√	×

5 电子档案真实性的保障

5.1 存证数据要求

a）存证的电子数据记录应有唯一的存证标识码。

b）存证的电子数据记录应包括存证的电子数据的完整性校验值及使用的完整性校验算法。

c）存证的电子数据记录应包括可信时间戳。

d）存证的电子数据记录应能和特定用户进行关联，即具有特定用户的签名信息。

e）存证的电子数据记录应包括完整的日志信息、存证过程中关键节点的可信时间戳、用户、操作内容、对象和存储路径等信息。

f）电子数据存证平台存证原文的，存证的电子数据记录应包括原文以及原文附属信息（a）-（e）。

g）分系统建议：

- 业务系统的存证数据建议包括：业务系统编码、系统名称、系统启用时间、操作人、操作时间、唯一编码、电子文件Hash等描述项；
- 档案管理系统的存证数据建议包括：业务编码、业务字段等业务数据；档号、归档时间、归档单位、保管期限、文件格式、提供利用等档案管理元数据；电子文件名称、唯一编码、电子文件Hash等元数据；
- 长期保存系统的存证数据建议包括：业务编码、业务字段等业务数据；档号、归档时间、归档单位、保管期限、文件格式、提供利用等档案管理元数据；电子文件名称、唯一编码、电子文件Hash等元数据。

h）应保存完整的可信时间戳证书，确保在离线环境下仍可进行独立的真实性验证。

5.2 存证场景

a）支持各类系统调用存证API接口存证，包括各类业务系统、各类档案管理系统、各类长期保存系统；

b）支持各类电子文件、电子档案及相关信息存证，如业务文档、日志文件、元数据、校验算法等；

c）支持单机存证场景、局域网存证场景、互联网存证场景以及混合部署的存证场景；

d）支持采用固化存储技术（如蓝光存储）对存证数据进行固化处理；

e）存证数据线下传输宜采用一次写入多次读取光盘作为存证数据载体。

6 电子档案真实性的验证

6.1 通用要求

a）应支持原文存证验证方式。电子数据存证服务使用者存证原文的，需要进行原文存证验证时，电子档案真实性保障系统应计算提交的电子数据原文的完整性校验值并进行验证。

b）应支持非原文存证验证方式。电子数据存证服务使用者不存证原文而存证原文完整性校验值等信息的，需要进行验证时，应把原文和完整性校验算法提交到电子档案真实性保障系统，电子档案真实性保障系统根据提交的原文和完整性校验算法计算完整性校验值，并在该使用者存证的完整性校验值中进行检索，根据检索结果进行验证。

6.2 验证场景

a）应支持单机存证场景下的验证。根据电子数据原文的完整性校验值、可信时间戳进行验证，判断电子数据是否未经篡改以及其真实性和完整性。

b）应支持局域网存证场景下的验证。根据电子数据原文的完整性校验值、可信时间戳、数字签名（如有）进行验证，判断电子数据是否未经篡改以及其真实性和完整性。

c）应支持互联网存证场景下的验证。根据电子数据原文的完整性校验值、可信时间戳、数字签名（如有）进行验证，判断电子数据是否未经篡改以及其真实性和完整性。

d）应支持混合部署场景下的验证。适应私有云、公有云、混合云架构，支持跨环境的验证流程。

e）支持各类系统对存证API接口的调用验证，涵盖各类业务系统、各类档案管理系统以及各类长期保存系统。

f）应支持自动化的批量验证，智能识别并报告异常。

6.3 验证结果

电子档案真实性保障系统应提供验证结果，验证结果包括但不限于：

a）存证标识码；

b）存证的电子数据的原文（如适用）；

c）存证的完整性校验值及使用的完整性校验算法；

d）可信时间戳；

e）存证用户信息；

f）存证日志信息。

7 第三方资质要求

第三方电子档案真实性服务平台资质应符合但不限于以下要求之一：

a）网络安全等级保护应符合GB/T 22239中第三级或更高级别要求；

b）部署在境内的公有云、互联网数据中心或自建机房；

c）具备国家密码管理局颁发的《商用密码产品认证证书》；

d）获得相关的信息安全管理体系的权威认证。

参考文献

[1] GB/T 18894-2016 电子文件归档与电子档案管理规范
[2] DA/T 92-2022 电子档案单套制管理一般要求
[3] DA/T 93-2022 电子档案移交接收操作规程
[4] DA/T 97-2023 电子档案证据效力维护规范
[5] SF/T 0076—2020 电子数据存证技术规范
[6] GB/T 25069-2010 信息安全技术 术语
[7] 最高人民法院关于民事诉讼证据的若干规定（2019修正）
[8] GB/T 20520-2006信息安全技术公钥基础设施 时间戳规范
[9] 中华人民共和国档案法（2021年1月1日起施行）
[10] 中华人民共和国档案法实施条例（2024年3月1日起施行）