ICS 35.240.01
A 16

SF

中华人民共和国司法行政行业标准

SF/T 0076—2020

电子数据存证技术规范

Technical specification for digital evidence preservation

2020－05－29 发布　　2020－05－29 实施

中华人民共和国司法部　　发布

目　　次

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

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这些专利的责任。

本标准由司法鉴定科学研究院提出。

本标准由司法部信息中心归口。

本标准起草单位：司法鉴定科学研究院、公安部第三研究所、厦门市美亚柏科信息股份有限公司、国家工业信息安全发展研究中心、中国科学院软件研究所、上海弘连网络科技有限公司。

本标准主要起草人：郭弘、施少培、吴松洋、王勇、潘妍、李岩、文静、丁丽萍、陆道宏、张鹤、卢建斌、钱志高、张辉极。

电子数据存证技术规范

1 范围

本标准规定了电子数据存证服务提供者、电子数据存证平台和电子数据存证过程的要求。

本标准适用于电子数据存证的规范化运作。

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。

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 35273—2020 信息安全技术 个人信息安全规范

GA/T 1568—2019 法庭科学 电子物证检验术语

3 术语和定义

GB/T 22239—2019、GB/T 35273—2020、GA/T 1568—2019界定的以及下列术语和定义适用于本文件。

3.1

电子数据存证 digital evidence preservation

通过互联网向用户提供电子数据证据保管和验证的服务。

3.2

电子数据存证服务提供者 digital evidence preservation provider

提供电子数据存证服务的机构或组织。

3.3

电子数据存证服务使用者 digital evidence preservation user

使用电子数据存证服务的组织或个人。

3.4

电子数据存证平台 digital evidence preservation platform

由电子数据存证服务提供者向使用者以网站、应用程序和编程接口等形式提供电子数据存证服务的软件或系统。

3.5

可信时间标识 trusted timestamp

唯一地标识某一刻时间的字符序列。

注：该标识不仅可以标识出行为的发生时间，还可以通过时间的先后顺序构建带时序的证据链条。

3.6

区块链 blockchain

一种在对等网络环境下，通过透明和可信规则，构建不可伪造、不可篡改和可追溯的块链式数据结构，实现和管理事务处理的模式。

注：事务处理包括但不限于可信数据的产生、存取和使用等。

[GB/T 37043—2018，定义2.5.8]

4 电子数据存证服务提供者

电子数据存证服务提供者应具备与服务规模相适应的技术人员和专业能力，并且具有完善的管理机制。

5 电子数据存证平台

5.1 系统安全

电子数据存证平台应达到GB/T 22239—2019的第三级基本要求。

5.2 运行环境安全

5.2.1 电子数据存证平台的系统或软件应7×24小时稳定运行。

5.2.2 电子数据存证平台存证数据所使用的物理设备及环境应有完善的监控体系。

5.2.3 电子数据存证服务提供者应采取措施保障电子数据存证平台的安全，预防非授权的访问或破坏。对于非授权的访问或破坏应具有防护措施和应急预案。

5.3 存储安全

电子数据存证平台应具备冗余备份和存储扩展的能力，并具备异地容灾能力。

5.4 通信网络安全

电子数据存证平台应定期检查，防止网络攻击、病毒和网络代理的使用。

5.5 数据安全

5.5.1 电子数据存证平台宜采用符合国家密码管理主管部门认证核准的密码技术对数据进行加密传输和存储，并对密钥采取必要的保护机制。

5.5.2 电子数据存证平台应承诺存储内容符合国家有关规定。

5.6 系统软件安全

电子数据存证服务提供者应保证电子数据存储和传输过程涉及的系统和软件完全可控，系统接口及系统配置安全可靠，避免系统代码被反编译或篡改。

5.7 数据可追溯

电子数据存证平台应确保所存证的电子数据可被验证和追溯。

5.8 时间可信

电子数据存证平台的系统时间及生成的可信时间标识应从国家可信时间源进行授时和守时。

5.9 系统对接

5.9.1 电子数据存证服务提供者提供编程接口与其他存证平台或应用系统进行对接时，应对接入的存证平台或应用系统进行评估，确保其符合本标准的要求。

5.9.2 电子数据存证服务提供者与法院、仲裁等其它电子数据存证平台或应用系统进行对接时，应符合对接部门的要求。

5.10 技术实现

电子数据存证平台可采用多种技术确保对电子数据的生成、收集、传输、存储和展示过程合法合规，采用的技术包括但不限于：

a) 可信计算技术；
b) 校验技术；
c) 数字签名技术；
d) 电子身份认证技术；
e) 可信时间戳技术；
f) 区块链技术；
g) 加解密技术；
h) 智能合约技术；
i) 分布式存储和计算技术；
j) 云计算和大数据技术；
k) 存储虚拟化技术。

6 电子数据存证过程

6.1 通用要求

6.1.1 电子数据存证前，电子数据存证服务提供者应对电子数据存证服务使用者进行身份核验。电子数据存证服务使用者宜检查存证使用的计算机信息系统的硬件、软件以及网络环境是否可靠、安全，并处于正常运行状态，条件允许时宜将相关信息也进行存证。

6.1.2 电子数据存证时，电子数据存证服务使用者使用电子数据存证服务提供者提供的网站、应用程序或编程接口，应将电子数据的原文或完整性校验值、附属信息等数据同步传输至电子数据存证平台。

6.1.3 电子数据存证服务提供者应记录电子数据存证平台的硬件设备信息、软件系统信息、网络信息及过程数据等，并计算相关信息的完整性校验值。将记录的数据与对应的完整性校验值同时进行存证。

6.1.4 电子数据存证服务使用者需要进行原文存证的，应提交电子数据原文到电子数据存证平台；电子数据存证服务使用者不需要进行原文存证的，电子数据存证平台应进行风险告知，避免使用者自己破坏完整性导致无法验证而产生纠纷。

6.2 存证数据

6.2.1 存证的电子数据记录应有唯一的存证标识码。

6.2.2 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。

6.2.3 存证的电子数据记录应包括可信时间标识。

6.2.4 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。

6.2.5 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标识、用户、操作内容、对象和存储路径等信息。

6.2.6 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附属信息。

6.3 存证数据传输

6.3.1 身份认证

电子数据存证服务使用者传输数据前，电子数据存证平台应对其身份进行可信认证，并保留认证记录。

6.3.2 加密传输

电子数据存证服务使用者和电子数据存证服务提供者的通信宜采用密码技术，保证传输过程中数据的保密性。

6.3.3 传输完整性验证

应采用校验技术对电子数据存证服务使用者和电子数据存证服务提供者的传输数据进行校验，确保传输数据的完整性。

6.4 存证数据验证和验证结果

6.4.1 存证数据验证

电子数据存证平台应提供多种验证方式，不论何种方式的存证，电子数据存证平台都应进行验证，并给出验证结果。电子数据存证平台的存证验证方式包括：

a) 原文存证验证

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，电子数据存证平台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) 非原文存证验证

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数据存证平台，电子数据存证平台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。

6.4.2 验证结果

电子数据存证平台应提供验证结果，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) 可信时间标识；

e） 存证用户信息；
f） 存证日志信息；
g） 其它附属信息。

6.5 数据检索

6.5.1 电子数据存证平台应向已认证的电子数据存证服务使用者提供通过数据关键词和时间等条件，对其提交的存证数据进行检索的服务。

6.5.2 电子数据存证平台不宜向未认证的电子数据存证服务者提供数据检索服务。

6.6 隐私保护

电子数据存证平台应符合GB/T 35273—2020要求，并符合以下要求：

a） 电子数据存证平台应仅采集和保存存证业务必需的用户个人信息；
b） 电子数据存证服务使用者可检索其提交的存证数据，检索结果可显示完整的存证信息；
c） 电子数据存证平台其他使用者的检索结果中不宜显示非其存证数据的存证信息；
d） 电子数据存证平台的管理员检索电子数据存证服务使用者的存证信息，所有的数据访问应被记录。检索结果不宜显示完整的存证信息，涉及到个人敏感信息的应进行去标识化处理。

参 考 文 献

[1] GB/T 20520—2006 信息安全技术 公钥基础设施 时间戳规范
[2] GB/Z 28828—2012 信息安全技术 公共及商用服务信息系统个人信息保护指南
[3] GB/T 29360—2012 电子物证数据恢复检验规程
[4] GB/T 29361—2012 电子物证文件一致性检验规程
[5] GB/T 29362—2012 电子物证数据搜索检验规程
[6] GA/T 756—2008 数字化设备证据数据发现提取固定方法
[7] GA/T 976—2012 电子数据法庭科学鉴定通用方法
[8] SF/Z JD0400001—2014 电子数据司法鉴定通用实施规范
[9] 中华人民共和国网络安全法，2017年6月1日
[10] 中华人民共和国密码法，2019年10月28日
[11] 中华人民共和国电子签名法，2019年4月23日
[12] 中华人民共和国档案法，2016年11月7日
[13] 中华人民共和国档案法实施办法，2017年3月1日
[14] 公安部网络安全保卫局，北京网络行业协会，公安部第三研究所.互联网个人信息安全保护指南，2019年4月10日
[15] 法释〔2018〕16号.最高人民法院关于互联网法院审理案件若干问题的规定，2018年9月6日
[16] 国家互联网信息办公室令第3号.区块链信息服务管理规定，2019年1月10日
[17] 可信区块链推进计划.区块链司法存证应用白皮书（v1.0），2019年6月