杭州互联网法院电子证据平台规范（试行）

第一章　总则

第一条 为规范电子数据的接入、传输、交换，完善杭州互联网法院电子证据平台的建设和管理，根据《中华人民共和国民事诉讼法法》《中华人民共和国网络安全法》等相关法律规定，结合本院改革试点审判实践，制定本规范。

第二条 本规范适用于接入平台的机构和其他组织。

第三条 证据平台符合安全性、高效性和可控性要求。

安全性是指数据哈希值在平台传输、保存过程中保持稳定性、安全性。

高效性是指平台具备广泛的应用基础和通用的应用标准，能够与其他技术体系实现快速的对接。

可控性是指法院完全掌控平台的运营，有效防止数据泄密，杜绝数据被不当使用。

第四条 规范中有关术语定义与解释：

电子证据：包括电子数据和其他诉讼证据的电子化。

杭州互联网法院诉讼平台（以下简称“诉讼平台”）：杭州互联网法院在线审理涉网纠纷的专业性平台，可用于存储、接入、交换、认证诉讼过程中形成的电子证据。

杭州互联网法院电子证据平台(以下简称“证据平台”)：杭州互联网法院通过接口对接方式,存储电子数据摘要、推送电子证据至诉讼平台的专业性平台。

电子数据摘要：即哈希值（HASH），是对文件内容数据通过逻辑运算得到的数值。

JSON：一种轻量级的数据交换格式，简洁和清晰的数据交换语言， 易于人阅读和编写，同时也易于机器解析和生成。

HTTP：超文本传输协议，是互联网上应用最为广泛的一种网络协议，所有的互联网资源都必须遵守这个标准。

RESTful：一种软件架构风格、设计风格，提供了一组设计原则和约束条件，基于这个风格设计的软件可以更简洁，更有层次，更易于实现缓存等机制。

电子签名：是指数字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。

时间戳：表示一份数据在某个特定时间之前已经存在的、完整的、可验证的数据,通常是一个字符序列，唯一地标识某一刻的时间。

数据加密：使用对称加密或非对称加密算法对电子证据进行加密处理，将明文数据改变为难以读取的密文内容。

第三方电子认证机构：取得国务院信息产业主管部门颁发的电子认证许可证书、提供电子签名认证服务的机构。

CA 证书：第三方电子认证机构签发的电子签名认证证书，用于实现对证书持有者身份的认证。

第三方数据持有者：与当事人无利害关系、电子数据在业务过程中自动落地并存储的机构。

第三方数据服务提供商：为当事人提供电子数据存证等服务的机构。

平台接入方：与证据平台通过接口实现对接、提供电子数据摘要导入的机构，包括但不限于第三方数据持有者、第三方数据服务提供商。

第五条 本规范基于以下文件制定:

中华人民共和国电子签名法；

GB/T 20520—2006 信息安全技术 公钥基础设施 时间戳规范；

GB 50174—2017 数据中心设计规范。

第二章　电子数据规范

第六条 根据接入平台的电子数据类型的不同，电子数据可分为公文电子数据和私文电子数据。

公文电子数据包括国家机关、事业单位等依职权形成的电子数据。

私文电子数据包括公证机构、第三方数据持有者、第三方数据服务提供商以及其他机构和个人持有的电子数据。

第七条 公文电子数据、公证电子数据、第三方数据持有者的电子数据可与证据平台通过接口实现对接，也可直接接入诉讼平台；其他私文电子数据应通过电子数据摘要验证方式先与证据平台通过接口实现对接。

第八条 证据平台接入方需向本院提供主体身份资料、联系方式等信息。本院管理员审核同意后，通过国家授权的第三方电子认证机构为其颁发 CA 证书，用于确保网上传递信息的机密性和完整性。

第九条 第三方数据服务提供商应具备可持续提供存证服务的能力，并且被市场有效验证，其连接证据平台开展司法电子证据服务，其用户（包括自然人、法人、非法人组织）应当通过严格的实名认证，认证方案不确定或存在瑕疵的，禁止接入。

第十条 平台接入方的系统或软件的运行环境应当符合国家标准，同时还应符合以下标准：

系统硬件安全：系统硬件应当确保由所有者或者使用者所完全控制，不能被非法用户所使用；系统硬件应当在 7*24 小时稳定可靠使用，不可抗拒原因除外；

系统存储：系统存储应当容量充足，长期使用率处于 70% 以下，并具备冗余备份能力；

系统时间：对于计算机、手机、手持电子设备，能够获取设备的本地时间，并且与国家授时中心的时差小于 2 秒；

系统网络信息记录：对于联网设备，软件应当能够获取该设备的所有本地网络地址与公网网络地址，以及域名服务器、网关、路由表等网络信息。

第三章　电子数据格式

第十一条 提交至证据平台的电子数据应当满足以下保管要求：

（一）能够有效表现所载内容；

（二）电子数据的格式与其生成、发送或者接收时的格式相同，或者格式不相同但是能够准确表现原来生成、发送或者接收的内容。

第十二条 通过证据平台导入诉讼平台的电子数据是基本单位的电子数据，不包括 Zip、RAR、7z 等压缩文件格式。

第十三条 基本单位的电子数据包括结构化数据和非结构化数据。

结构化数据即行数据,可以用二维表结构来逻辑表达实现的数据。

非结构化数据指字段长度可变且每个字段的记录又可以由可重复或不可重复的子字段构成的数据，包括常用的办公文档、文本、图片、网络页面、报表、音频和视频信息等。

第十四条 第三方数据服务提供商除固定业务数据外，还可固定业务数据的处理流程数据、物理电子设备标识和其他信息。

处理流程数据包括并不限于运行环境数据、运行日志、用户操作记录、系统管理记录等数据。

物理电子设备标识包括但不限于中央处理器序列号、主板序列号、磁盘序列号、网卡序列号或网卡的物理地址、手机等移动设备的 IMEI 或 UUID 等标识。

其他信息包括但不限于主体信息、采集时间、地点、手段、方式等信息。

第四章　电子数据的保障及技术规范

第十五条 平台接入方应采取一种或多种方式保障电子数据的完整性、有效性、不可篡改性和清洁性。

第十六条电子数据可生成电子数据摘要用于作为标识该条记录的唯一值，可通过时间戳、电子签名、分布式多可信节点同步等方式进行固定和防篡改，传输荷载可经由非对称加密算法进行加密后传输，或通过加密通讯协议传输数据，也可通过其他可信方式进行固定和保障。

第五章　电子数据标准接口规范

第十七条证据平台接口遵循如下设计原则：

开放：面向社会所有相关组织与单位，能够对接各个行业多种类型的接入者。

标准：平台制定了接入规范与标准的通讯协议，目标是整个系统的所有子系统与模块之间通过标准的技术与接口进行通讯。

兼容：通讯协议支持 HTTP 网络传输协议，也能够支持未来其它的传输协议，能够兼容所有软件系统与流行的互联网通讯协议风格。

市场主流：平台使用目前市场主流的 JSON 为主要的数据格式，并使用基于非对称加密的访问令牌验证。

第十八条传输数据格式包含 HTTP+JSON 文本格式和 HTTP+二进制数据包形式。

二进制数据包的数据格式包括：起始标识、包长字段、标识字段、元信息段、包体长度、包体、检验字段等。

第十九条所有接入者与证据平台的通讯均采用请求应答模式，消息通讯使用互联网常用的 RESTful 模式，请求与应答消息包以 JSON 格式为主。

第二十条接入者在接入证据平台前，需要接入者提供获取会话令牌接口和鉴权密钥，经证据平台验证通过方可建立会话。

第六章　司法应用

第二十一条平台接入方将电子数据的电子数据摘要存入证据平台后，当事人及其诉讼代理人应遵循以下司法应用过程：

1.当事人及其诉讼代理人在诉讼平台输入存证编号；

2.诉讼平台向第三方数据服务提供商发出调取指令；

3.第三方数据服务提供商根据存证编号和当事人主体信息进行检索，将同时符合存证编号和当事人主体信息的电子数据，推送至证据平台；

4.证据平台对接收的电子数据通过电子数据摘要自动比对，核验无误后导入诉讼平台。

第七章　附则

第二十三条 本规范由杭州互联网法院负责解释。

第二十四条 本规范自 2018 年 6 月 28 日起施行。