电子证据保全服务等级协议

本服务等级协议（以下简称“协议”或“SLA”）规定了用户与北京数字认证股份有限公司（以下简称“数字认证公司”或“本公司”）电子证据保全服务（以下简称“服务”）可用性等级指标和相关服务方案。

1. 术语和定义

1.1. 云服务

云服务是指数字认证公司提供的基于云计算技术架构的互联网信息化服务。

1.2. 用户

用户（也称“客户”）是指从数字认证公司购买电子证据保全服务的主体。

1.3. 时间戳

对时间和其他待签名数据进行签名得到的数据，用于表明数据的时间属性。

1.4. 哈希算法

又称杂凑算法、密码散列算法。该算法将一个任意长度的比特串映射到一个固定长的比特串，且满足下列三个特征：

1） 为一个给定的输出找出能够映射到该输出的一个输入是计算上困难的；

2） 为一个给定的输入找出能够映射到同一个输出的另一个输入是计算上困难的；

3） 要发现不同的输入映射到同一输出是计算上困难的。

1.5. 数字签名

数字签名是一种基于公钥密码技术的电子签名实现方式，签名者使用私钥对待签名数据的杂凑值做密码运算得到的结果，该结果只能用签名者的公钥进行验证，用于确认待签名数据的完整性，签名者身份的真实性和签名行为的抗抵赖性。

1.6. 电子证据保全

电子证据保全是指对于可能灭失或者以后难以提取的电子证据，通过技术手段采取一定的措施先行加以固定和保护，以便事后证明待证事实。

2. 服务内容

2.1. 电子证据保全服务

数字认证公司为用户提供的电子证据保全服务是对电子数据采用时间戳和电子签名技术进行可信的固化处理并进行一定期限的安全存储和事后出证的服务。

电子证据保全服务可以为多种电子数据形式提供保全服务，服务提供 SDK 供用户业务系统进行原始电子数据的哈希处理。

2.2. 服务形式

本公司提供的电子证据保全服务为公有云模式调用，用户业务系统通过调用公有云保全服务 API 接口完成保全服务请求。

2.3. 服务用量

电子证据保全服务以文件作为电子数据集合计量单位，服务的使用数量按照文件数量计算。用户业务系统调用电子证据保全服务接口为一个电子数据文件或文件电子摘要进行数字签名、时间戳固化，并存储为一个保全文件的过程即记为新增一个保全用量。用户业务系统在电子证据保全服务系统内存储的所有有效保全文件即为在用保全用量。用户业务系统在计费约定时限范围内系统内累积存储的在用保全用量即为服务用量。

3. 服务范围

3.1. 集成对接

数字认证公司提供电子证据保全服务的集成对接包括电子证据保全服务 SDK 对接支持、服务公测平台集成、服务上线支持和相关过程集成咨询。

用户购买电子证据保全服务时，数字认证公司即向用户提供云服务公测平台集成服务，用户业务

系统可以在公测平台完成云服务接口集成验证。用户在电子证据保全服务购买期限内随时可以使用该公测平台验证用户业务系统与云服务接口对接的正确性。

用户完成公测平台验证后，使用正式授权参数配置即可接入云服务生产平台，但服务只能在服务开通后才能正式调用。

用户业务系统集成开发过程中，数字认证提供必要的 API、服务组件及配套集成开发指南和相关工具，用户集成过程中的问题可通过电话、微信、QQ 等方式获得技术支持。

3.2. 服务开通

数字认证公司根据与用户约定的服务开通日开电子证据保全服务，服务开通之日起用户即可正式使用该服务，服务计费也即时开始。

用户应确保在服务开通之前已完成与云服务接口的对接，并按照正确的配置使用服务。

3.3. 服务计费

电子证据保全服务按照套进行购买，每套包含每年 10 万个保全文件。用户可以根据业务实际情况选择购买多套服务。每套服务期限为 1 年，从数字认证公司为用户开通电子证据保全服务之日起开始计费，服务期限届满后，用户可用保全文件数量自动清零。

若服务期限届满前，用户已达到购买的文件数量的，视为数字认证公司已履行完毕服务约定，用户将无法继续增加保全文件数量。

电子证据保全服务提供多种模式的服务，每种模式的价格均不同，具体价格以用户和数字认证公司签订的合同为准。

3.4. 服务维护

数字认证公司保障用户在订购服务服务期限内正常使用服务功能，并提供以下服务维护：

(1) 服务关联组件的升级服务：用户可以通过公开网站、本公司指定项目经理等途径获取最新的关联组件版本，并自行在其业务系统中进行升级更新；

数字认证公司发布的新版服务关联组件，建议用户及时更新，对于已退出数字认证公司组件维护清单的旧版服务关联组件，将不再提供后续的维护服务。

(2) 服务修正和改善的升级：数字认证公司发现提供的服务存在错误或需要进行改善时，会对服务进行更新升级修正，避免因错误引起用户利益损失，提高服务体验。

3.5. 服务告知

当数字认证公司可能知悉如下事项的发生会对电子证据保全服务产生影响时，将至少提前 3 个工作日，以网站公告或电子邮件方式告知用户。包括但不限于：

(1) 任何中止或终止用户使用服务的情形；

(2) 在进行平台配置、维护、升级时，需要短时间中断服务的情形；

(3) 计划的平台配置、维护、升级时间需要变更的情形。

因上述突发性事件对电子证据保全服务产生影响时，数字认证公司不承诺一定能够提前 3 个工作日进行通知。

3.6. 客户服务

数字认证公司云服务提供热线电话、在线服务和自助服务等方式，方便用户随时获得技术支持。

热线电话快速响应用户需求，指导用户相关工程师进行操作，确保用户的问题能够得到及时准确的反馈。

在线服务通过微信公众号、微信群、电子邮件等远程服务方式进行，借助互联网能力更方便地支持客户问题的及时准确的反馈。

客户自服务模式为用户提供服务情况查询功能，用户能够自助浏览、检索常见问题的解决方案。

3.7. 服务资源配置

电子保全服务采用公有云服务架构，具备良好的弹性扩容和伸缩能力。客户业务日常压力变化无需关注云服务资源配置的变化，云服务会自动监测服务资源变化情况并主动进行运行资源和网络资源的调整。

客户业务存在连续指数级规模的巨大业务请求量变化时，考虑到大量资源配置调整生效的时延性，宜提前 7 个工作日向数字认证公司书面申请，以便资源配置及时调整到位满足巨量业务突发增长的要求。

对于采取专线等模式接入云服务的客户，由于网络资源的调整受基础网络运营商制约，应提前与数字认证公司协商确定资源配置调整生效周期。

3.8. 服务故障响应

数字认证公司制定完善的运维保障体系，具备先进的运行服务状态监测能力，并配备专业的运维人员 7x24 小时实时保障。数字认证公司可通过多种故障恢复手段及时修复运行过程中可能出现的问

题，保障服务及时恢复正常。

当发生不在日常故障处置范围的严重故障时，将启动应急响应机制，进行服务的紧急恢复。

数字认证云服务具备同城服务容灾恢复和异地数据容灾恢复能力，在发生灾难事件时将启动容灾切换机制，进行服务恢复。

个别用户或区域出现服务故障时，数字认证公司通过客户咨询服务提供相关故障恢复的帮助。

4. 服务等级指标

4.1. 服务时效性

数字认证公司对电子证据保全服务时效性做如下承诺：

服务类型	服务时效
集成对接	按合同承诺期限完成
公测服务	7×24 小时实时调用
服务开通	按合同约定期限完成
生产服务	7×24 小时实时调用
服务维护	7×24 小时
客户服务	人工呼叫 5×8 小时受理，客席接入率 90%
	在线自助 7×24 小时
服务扩容	60 分钟内完成应用服务能力 50%扩展 15 分钟内完成应用服务能力 10%扩展
服务故障响应	服务故障 15 分钟内启动响应，2 小时内确定故障并解决。需要启动容灾响应的，在启动后 2 小时完成容灾切换

4.2. 服务可用性

电子证据保全服务可用性指标不低于 99.95%，按如下公式计算。

电子证据保全服务可用性 = 每服务周期可用时间 /（每服务周期可用时间 + 每服务周期不可用时间）*100%

其中：

(1) 电子证据保全服务的服务可用性核算界定的每服务周期为一个自然月，自服务开通之日起计算，不满一个月按照一个服务周期计算。

(2) 每服务周期可用时间：现网用户 90%以上可以正常获得服务响应即视为服务可用。

(3) 本公司预先通知的计划内升级扩容维护等引起的短时服务中断，不计入不可用时间。

(4) 因用户设备、网络故障等原因造成的服务不可用，不计入不可用时间。

(5) 因用户自身业务系统升级改造等原因造成的服务无法正常使用，不计入不可用时间。

(6) 因第三方供应商原因（云服务提供商、网络供应商等）造成的服务不可用，不计入不可用时间。

4.3. 数据持久性

电子证据保全服务数据持久性不低于 99.99999999%。

电子证据保全数据持久性按照数据保存周期统计，一个保存周期为一个自然月，不满一个月按照一个月计算。即每 10,000,000,000 份保全文件，每月最多有 1 份文件丢失。

4.4. 数据可销毁性

数字认证公司对用户非必须保存的个人信息进行销毁，不再另行通知用户。销毁方式和技术手段，符合数据销毁的安全要求并留存操作事件记录。

4.5. 数据可迁移性

数字认证公司保全服务平台存储的用户保全文件具备数据可迁移性，用户在服务期限内可随时通过服务接口提取数据并自行迁移。

4.6. 数据知情权

数字认证公司保全服务存储保全数据存储位置和备份情况具有知情权。

当前电子保全服务数据存储在阿里云（北京城区），在同城 10 公里以上建立备份数据中心，实现同城双活。

电子保全服务数据备份自动执行，用户不能指定存储位置，也无需关注。

除非满足服务可审查性要求，数字认证公司不会将用户数据和访问记录提供给第三方。

4.7. 服务可审查性

依据现行法律法规或根据政府监管、安全合规、审计或取证调查等原因的需要，在符合流程和手续完备的情况下，本公司可以向申请部门或单位提供用户所使用的服务的相关信息，包括但不限于请求记录、关键组件的运行日志、运维人员操作记录、用户操作记录等信息。

4.8. 数据私密性

本公司通过有效的身份鉴别手段确认用户业务服务的身份，采用密码技术对用户的业务服务身份进行可信认证，为用户业务的数据提交、查询、下载等各环节提供身份安全保障。

此外，在调用电子证据保全服务时，本公司通过 https 安全信道、密文方式传输用户的保全请求和保全数据，防止数据被截取、篡改。

本公司建立严格的运维管理制度，禁止运维人员接触业务数据，且通过堡垒机记录和审查运维人员的操作记录，相关业务敏感数据均采取加密方式存储，运维人员无法查看原文。

本公司不会主动查看用户的数据，除非适用第 4.4 条之服务可审查性规定的情况，这些操作要经过内部审批流程，由运维人员在堡垒机上操作并进行日志记录。

4.9. 服务计量准确性

数字认证公司电子证据保全服务平台具备准确的计费统计系统，根据用户实际服务用量进行结算并扣费，具体计费标准以合同约定的计费模式与价格为准，计费数据保留不少于 1 年。

4.10. 服务可靠性

电子证据保全服务基于云化硬件网络基础设施架构，具备良好的弹性扩展和冗余部署能力，确保平台内无单点运行风险。

此外，数字认证公司建立完备的数据备份机制，确保在发生不可控风险时，在合理范围内恢复服务数据。

4.11. 故障恢复能力

数字认证公司具备 7*24 小时的系统运维能力，具备完善的故障监控、自动告警、快速定位、快速恢复等一系列故障应急响应机制，有效保障电子证据保全服务的正常运行。

当电子证据保全服务发生故障时，数字认证公司启动相应的响应措施，及时恢复业务。

5. 服务赔偿条款

5.1. 服务赔偿范围

因数字认证公司电子证据保全服务故障导致用户无法使用约定的服务并对用户业务产生实质性

损失时，用户可以提出赔偿申请。由于以下原因所导致的服务不可用本公司不承担赔偿责任：

(1) 数字认证公司预先通知的系统维护所引起的，包括系统升级、维护和故障模拟演练；

(2) 用户的网络、设备故障或配置调整引起的；

(3) 本 SLA 第 7 条免责条款中约定的情况引起的；

(4) 其他非数字认证公司原因所造成的。

5.2. 赔偿方案

数字认证公司核查无误后，按照合同中约定的赔偿条款进行赔偿。若合同内未约定相关条款，将将按照当月用户服务不达标情况的严重程度，提供免费文件数量赔偿，但最多不超过当月新增保全文件数量。

数字认证公司按照服务可用性下降造成客户业务损失程度的大小进行分类赔偿，赔偿以免费赠送文件数量的方式进行，所有赔付的免费赠送文件数量在送达客户帐户之日起一个自然年内有效。

可用性区间	最大停止服务时间	赔偿次数计算
低于 99.95%，高于 99.5%	最长停服时间≤30 分钟	按照当月新增保全文件数量提供免费次数，最低不少于 2%，最高不超过 5%
低于 99.5%，高于 98%	最长停服时间≤120 分钟	按照当月新增保全文件数量提供免费次数，最低不少于 5%，最高不超过 10%
低于 98%	最长停服时间不小于 300 分钟	按照当月新增保全文件数量提供免费次数，最低不少于 10%，最高不超过 25%

6. 用户约束条款

(1) 用户应提供必要的部署环境、工作条件和设备条件（包括但不限于网络设备服务器、工作站、打印机、系统证书应用产品等运行环境），以便于电子证据保全服务的开通和使用。

(2) 用户应遵循数字认证公司产品集成文档或集成建议。

(3) 用户应在合法范围内使用合同中的产品及服务。

(4) 用户应按期足额缴纳相关服务费用。

(5) 数字认证公司拥有电子证据保全产品及服务的知识产权，用户不得复制、合并、修改、改编、反向编程产品及服务的全部或者任意部分；

(6) 用户应在约定范围中使用合同中的产品及服务。

(7) 用户应在约定范围中使用公测平台，亦不应在公测平台进行压力测试等操作。

7. 免责条款

（1）鉴于计算机、互联网的特殊性，下述情况不属于数字认证公司违约：

a. 非数字认证公司原因导致，数字认证公司未能按合同约定的时间提供产品或服务；

b. 数字认证公司在平台配置、维护、升级时，需要短时间中断服务；

c. 由于 Internet 上的通路阻塞造成用户业务系统访问服务速度下降；

d. 因第三方服务提供者的原因，造成服务不可用；

e. 不可抗力及意外事件引起的服务不能正常使用，例如自然灾害、战争、恐怖行为、政府司法行政机关的命令等。

（2）在如下情况，数字认证公司有权中止、终止对用户提供部分或全部服务而不承担任何责任：

a. 用户未按期或未足额缴纳服务费，双方达成一致可以中止、终止服务的情况；

b. 发现用户利用服务从事违法活动；

c. 其他数字认证公司认为需要中止、终止服务的情况。

（3）因用户未及时更新服务组件，导致服务不可用或其业务系统服务受损等情形，数字认证公司不承担任何责任。

（4）在对接测试期间，数字认证公司不对任何服务可用性、可靠性做出承诺，亦不对用户使用本服务的工作或结果承担任何责任。

8. 协议变更、终止条款

数字认证公司会适时修改 SLA，但在用户服务订购期限内，以用户签订合同时数字认证公司公布的 SLA 的版本为准；如果用户续订服务，则适用续订之时公布的 SLA 版本。

适用于第 7 条免责条款第（2）款的场景时，该协议将自动终止，且数字认证公司不承担任何责任。