

# 个人协同签名服务等级协议

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”）个人协同签名服务（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”）是从数字认证公司购买个人协同签名服务的主体。

### 1.3. 电子签名

电子签名是指数据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。

### 1.4. 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。

### 1.5. 数字证书

数字证书指由电子认证服务机构（CA）签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息的一种数据结构。

### 1.6. 证书持有者

证书持有者是通过 APP/小程序等移动端应用获得数字证书，在用户业务系统中使用数字证书的自然人。证书持有者在申请和使用数字证书过程中应遵守数字认证公司公布的相关业务规则与协议。

## 1.7. 服务套餐

服务套餐是指在一个自然年周期内用户按照不同的服务计费模式，使用服务相关功能接口的服务付费模式。

## 2. 服务内容

### 2.1. 个人协同签名证书服务

数字认证公司以云服务方式提供个人协同签名证书服务，服务内容涵盖身份核验和证书签发过程。其中身份核验是指本公司或本公司授权的注册机构对用户身份进行审核的过程，证书签发是指为已通过身份验证的证书持有者签发数字证书的过程。

### 2.2. 个人协同签名服务

个人协同签名服务是指用户业务系统请求个人协同签名服务，个人协同签名服务与证书持有者移动端协同对业务数据计算完成签名和签章，并由用户业务系统获取结果的过程。

个人协同签名服务依赖于数字证书完成数字签名，在进行数字签名前，证书持有者应先获取数字证书。

### 2.3. 服务形式

本公司提供的个人协同签名服务支持公有云模式和混合云模式。

在公有云模式下用户业务系统调用公有云服务 API，证书持有者通过使用 APP/微信小程序等移动端应用中的证书与公有云服务协同运算完成签名和签章服务。

在混合云模式下用户业务系统通过调用本地部署的签名认证网关使用公有云服务完成签名和签章服务，与公有云不同的是签章工作是在签名认证网关内部完成的。证书持有者与公有云服务的协同运算过程与公有云模式一致。

本公司提供 APP/微信小程序供用户使用，用户可以直接使用 APP/微信小程序完成证书下载和签名服务。如需个性化应用服务可以使用移动端 SDK 自行开发 APP 完成。

### 2.4. 服务用量

个人协同签名服务按照签名次数或协同签名用户数量的方式统计用户服务用量。

按照签名次数的计量方式是指用户业务系统调用个人协同签名服务接口完成签名过程即记为使

用完毕一次签名用量，用户业务系统在约定时限范围内累积使用完毕的签名用量即为用户服务用量。

按照协同签名用户数量的计量方式是指用户业务系统每创建一个自然人账户即记为使用完毕一个用户用量，用户业务系统在时限范围内累积使用完毕的用户用量即为用户服务用量。

### 3. 服务范围

#### 3.1. 集成对接

数字认证公司提供个人协同签名服务的集成对接包括移动端 SDK 对接支持、服务公测平台集成、混合云本地签名认证网关集成部署、服务上线支持和相关过程集成咨询。

用户购买个人协同签名服务时，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，但只能在服务开通后才能正式调用。

用户使用混合云本地签名认证网关集成服务时，数字认证公司可提供专业的集成实施人员支持用户现场软、硬件设备部署和联调测试。

用户业务系统集成开发过程中，数字认证提供必要的 API、SDK 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通个人协同签名服务，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

数字认证公司为用户提供阶梯模式的服务套餐供用户选择，用户可以根据业务实际用量选择购买套餐服务。

(1) 按签名次数购买的服务套餐最低 1 万次起购，按照阶梯模式享有不同的订购价格，用户最终确定的阶梯价格以数字认证公司与用户签订合同内容为准。服务套餐期限为 1 年，从数字认证公司为用户开通个人协同签名服务之日起开始计费，服务期限届满后若套餐内仍有未使用的服务次数，则剩余次数自动归零，且数字认证公司对于未使用完毕的服务次数不予退款。

若服务期限届满前，用户已使用完毕服务次数的，视为数字认证公司已履行完毕服务约定，服务自动终止。

(2) 按用户数量购买的服务套餐最低 1 千户起购，按照阶梯模式享有不同的订购价格，用户最终确定的阶梯价格以数字认证公司与用户签订合同内容为准。服务套餐期限为 1 年，从数字认证公司为用户开通个人协同签名服务之日起开始计费，服务期限届满后若套餐内仍有未使用的服务次数，则剩余次数自动归零，且数字认证公司对于未使用完毕的服务次数不予退款。

若服务期限届满前，用户已使用完毕服务次数的，视为数字认证公司已履行完毕服务约定，服务自动终止。

### 3.4. 服务维护

数字认证公司保障用户在服务期限内正常使用服务功能，并提供以下内容的维护服务：

(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) 服务错误修正和服务改善的升级：数字认证公司发现提供的服务存在错误或对服务进行改善时，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) APP/小程序的升级服务：本公司会定期通过应用商店对 APP/小程序进行升级维护。数字认证公司发布的新版本 APP 小程序，建议证书持有者及时更新。

### 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个人协同签名服务产生影响时，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；
- (4) 套餐有效期届满或套餐内服务数量使用完毕时。

因上述突发性事件对个人协同签名服务产生影响时，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。

热线电话快速响应客户需求，指导客户相关工程师进行操作，确保客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。

对于采购混合云软件的客户，数字认证提供远程和现场服务。当出现软件问题时，用户可以通过客户经理获得技术工程师的远程协助，如需现场解决的提供现场技术工程师服务。对于超过维保期限的，数字认证公司收取相应服务费用。

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

### 3.7. 服务资源配置

个人协同签名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

数字认证公司对个人协同签名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
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，混合云软件 5×8 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. 服务性能

个人协同签名服务按照公有云服务模式设计，支持动态并发压力扩充，服务性能在并发压力未触发动态扩容操作时平均服务处理时间不大于 100ms，最长处理时间不超过 3s。

服务处理时间为用户业务系统访问云服务，服务接口的响应时间。不包括请求从用户业务系统到达和离开云服务接口的数据网络传输时间以及等待业务 APP 扫码的时间。

服务动态扩容期间平均服务处理时间可能大于 100ms，但不超过最长处理时间，扩容完成后即恢复正常。

### 4.3. 服务可用性

个人协同签名服务可用性指标不低于 99.95%，按如下公式计算：

个人协同签名服务可用性 = 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) 个人协同签名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) 每服务周期不可用时间：每服务周期不可用时间 = 签名服务不可用时间+协同签名证书服务不可用时间。

(3) 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。

(4) 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。

(5) 因用户设备、客户端组件、客户网络、软件（网关）故障等原因造成的服务不可用，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。

#### 4.4. 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。

#### 4.5. 数据私密性

本公司云服务依照密码管理体系的要求，采用自主设计和实现的密钥管理体系和认证授权体系等手段保证用户数据私密性，即只有符合认证安全要求的用户业务系统，才能提交和获取该用户签名相关的业务数据，各用户业务系统无法获取其他用户的签名相关业务数据。

在调用个人协同签名服务时，本公司通过如下安全措施保障服务接口安全：

(1) 通过 https 安全信道、密文方式传输用户的签名请求和签名数据，防止数据被截取、篡改。

(2) 对用户的签名请求报文中的签名和应用 ID 进行校验，确保该签名请求通过了用户的授权。

在使用本公司提供的 APP 小程序调用云服务过程中，数字认证公司采用安全技术手段保障数据在互联网中的传输安全。

本公司协同签名技术仅在证书申请和使用过程中，提取用户口令参与相关密码计算过程，不会对证书持有者在身份认证和数字签名时使用的口令进行保存。

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用脱敏方式存储，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。

## 4.6. 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。

## 4.7. 数据隐私性

本公司承诺数字证书申请时仅采集签发数字证书所需的个人信息,符合《中华人民共和国网络安全法》、《GB/T35273-2020 信息安全技术个人信息安全规范》中的个人信息安全基本原则。数字认证公司制定并在网站 <http://www.bjca.cn> 公开发布的《个人信息保护政策》确保用户个人信息数据安全。

## 4.8. 服务计量准确性

数字认证公司个人协同签名服务平台具备准确的计量计费统计系统,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。

## 4.9. 服务可靠性

个人协同签名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。

## 4.10. 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,有效保障个人协同签名服务的正常运行。

当个人协同签名服务发生故障时,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

因数字认证公司个人协同签名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。在用户提出赔偿申请后，数字认证公司同意按照《北京数字认证股份有限公司电子认证业务规则》承担赔偿责任，但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，将按照当月用户服务不达标情况的严重程度，根据客户订购服务模式分别提供免费次数和免费服务时长，其中免费次数不多于每月平均服务次数，免费服务时长不大于一个月。

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，赔偿以免费赠送服务次数/免费服务时长的方式进行，所有赠送的免费服务次数/免费服务时长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	按次订购客户（不含不限次包年客户），按照客户年购买阶梯分档提供免费次数，最低不少于 1%，最高不超过 2.5%
		按用户数订购客户和不限次包年客户，统一提供免费延长使用时间，最低不少于 1 天，最高不超过 3 天
低于 99.5%，高于 98%	最长停服时间≤120 分钟	按次订购客户（不含不限次包年客户），按照客户年购买阶梯分档提供免费次数，最低不少于 3%，最高不超过 6%
		按用户数订购客户和不限次包年客户，统一提供免费延长使用时间，最低不少于 5 天，最高不超过 10 天
低于 98%	最长停服时间不小于 300 分钟	按次订购客户（不含不限次包年客户），按照客户年购买阶梯分档提供免费次数，最低不少于 7%，最高不超过 8.5%
		按用户数订购客户和不限次包年客户，统一提供免费延长使用时间，最低不少于 10 天，最高不超过 20 天

## 6. 用户约束条款

- (1) 用户知晓数字证书用于进行电子签名，并认可电子签名与手写签名或盖章具有同等法律效

力。同意由本公司为您提供数字证书的电子认证服务。

(2) 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），以便于个人协同签名服务的开通和使用。

(3) 用户应遵循数字认证公司产品集成文档或集成建议。

(4) 用户应在合法范围内使用个人协同签名服务。

(5) 用户应按期足额缴纳相关服务费用。

(6) 数字认证公司拥有个人协同签名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。合同中存在相关约定的情况除外

(7) 用户应在约定范围中使用合同中的产品及服务。

(8) 用户应当在其业务系统中或业务单证中明确告知数字证书申请者由数字认证公司向其提供电子认证服务，在数字证书申请者同意采用电子认证服务及电子签名的前提下，方可向数字认证公司提供符合要求的数字证书申请资料及信息。

(9) 用户应当在其业务系统中或业务单证中明确告知数字证书申请者同意并授权数字认证公司向其合作的可信身份数据源服务商传递与核实提交的身份信息。

(10) 用户自行进行身份核验时，需确保身份、申请资料及信息的真实、完整、准确，并承担相关责任。

(11) 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。

(12) 用户保证向本公司提交证书申请前，已获得证书申请者合法、有效且充分的授权。用户应妥善保管授权文件以备查。因用户超出授权范围或违法使用个人信息造成证书申请者投诉或追究的，用户应承担全部责任，由此给本公司造成经济损失的，用户应负责赔偿。

## 7. 免责条款

(1) 鉴于计算机、互联网等的特殊性，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。

(5) 证书申请者或用户故意或无意地提供了不完整、不可靠或已过期的信息，又根据正常的流程提供了必须的审核文件，得到了本公司签发的数字证书，本公司不承担与证书内容相关的法律和经济责任，但可以根据请求提供协查帮助。

(6) 本公司已谨慎地遵循了国家法律、法规规定的数字证书认证业务规则，而仍有损失产生的，本公司不承担赔偿责任。

## 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，本协议将自动终止，且数字认证公司不承担任何责任。