身份核验（API）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”）身份核验服务（API）（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身份核验服务（API）的主体。

1.3. 信息主体

信息主体是指信息所标识或者关联的自然人或组织。

1.4. 第三方合作机构

第三方合作机构是指经法律、行政法规许可或政府机关授权的，合法存有个人身份信息、实名手机号信息、银行账户信息、企业及法定代表人身份等信息的机构，包括但不限于公安部“互联网+”可信身份认证平台、“查询中心”等机构。

1.5. 身份核验

身份核验是在用户征得信息主体的授权同意后，本公司将信息主体提供的身份信息传递至第三方合作机构，并将第三方合作机构返回相关信息的一致性验证的评价结果及其他相关结果如实反馈给向信息主体提供产品或服务的用户业务机构的过程。身份核验的结果仅作为用户向信息主体提供商品或服务的参考。

1.6. 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. 个人身份核验服务（API）

个人身份核验服务（API）是指用户采集信息主体的姓名、身份证号、人像照片、手机号、银行卡号等信息中的一项或多项，并由数字认证服务送达第三方合作机构，并比对信息是否一致，来验证个人身份。包括但不限于证件信息核验、证件信息及人像的组合核验、手机号核验、银行卡核验等。

数字认证公司提供多种核验模式供用户选择，不同模式的身份核验对应的服务价格和性能存在一定差异，具体以用户实际购买服务为准。

2.2. 企业身份核验服务（API）

企业身份核验服务（API）是指用户采集企业的工商信息、法定代表人身份信息、企业的对公银行账号信息中的一项或多项，并由数字认证服务第三方合作机构，比对信息是否一致，来验证企业身份。包括但不限于企业工商信息核验、企业及法定代表人信息核验、企业对公银行账号核验等。

数字认证公司提供多种核验模式供用户选择，不同模式的身份核验对应的服务价格和性能存在一定差异，具体以用户实际购买服务为准。

2.3. 服务形式

本公司提供的身份核验服务（API）为公有云模式。用户业务系统通过公有云服务 API 调用完成身份核验服务。

2.4. 服务用量

身份核验服务（API）按照消耗核验次数的方式统计用户服务用量，用户业务系统调用身份核验服务接口并获得了身份核验服务返回结果即记为使用完毕一个核验用量，用户业务系统在约定时限范围内累积使用完毕的核验用量即为用户服务用量。

3. 服务范围

3.1. 集成对接服务

数字认证公司提供身份核验服务（API）服务的集成对接包括 API 接口的对接支持、服务上线支持和相关过程的集成咨询。

在集成对接过程中，数字认证公司提供一定数量的免费核验次数用于集成验证，免费核验次数能够满足用户集成对接验证要求。如果需要更多的免费集成验证次数请与您的销售专员联系申请。

用户业务系统集成开发过程中，数字认证提供必要的 API 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身份核验服务（API），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用供用户选择，用户可以根据业务实际用量选择购买服务套餐。

身份核验服务（API）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身份核验服务（API）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订购服务期限内正常使用服务功能，并提供以下维护服务：

(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。

3.5. 服务告知

当数字认证公司可能知悉如下事项的发生会对身份核验服务（API）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指定联系人。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) 因第三方平台资源配置调整造成服务能力下降的情形；

(4) 计划的平台配置、维护、升级时间需要变更的情形；

因上述突发性事件和可信数据源对身份核验服务（API）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。

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

身份核验服务（API）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。

受可信数据源的资源配置伸缩能力制约，当客户业务量突发增长时，可能无法及时扩展资源，从而影响本服务的性能。

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

数字认证公司对身份核验服务（API）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
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

身份核验服务（API）按照公有云服务模式设计，支持动态并发压力扩充，不同的身份核验模式服务性能存在一定差异，在并发压力未触发动态扩容操作时平均服务处理时间在 300ms 到 1200ms 之间。

服务处理时间为用户业务系统调用身份核验服务（API）时，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。

服务动态扩容期间平均服务处理时间可能大于上述时间，扩容完成后即恢复正常。

4.3. 服务可用性

身份核验服务（API）的可用性指标不低于 99.9%，按如下公式计算。

身份核验服务（API）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) 身份核验服务（API）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、业务系统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) 因用户违反第三方供应商（电信运营商、网络供应商等）协议造成的服务不可用，不计入不可用时间。

(7) 因第三方供应商原因（云服务提供商、网络供应商、可信数据源提供方）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

在调用身份核验服务（API）时，本公司通过 https 安全信道、密文方式传输用户的身份核验请求和核验结果数据，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

本公司承诺身份核验服务在进行用户个人信息的传输过程中，符合《中华人民共和国网络安全法》、《GB/T 35273-2020 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

数字认证公司身份核验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

身份核验服务（API）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，有效保障身份核验服务（API）的正常运行。

当身份核验服务（API）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

因数字认证公司身份核验服务（API）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，将按照当月用户服务不达标情况的严重程度，提供免费服务次数赔偿，但最多不超过原合同每月平均服务次数。

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的方式进行，所有赔付的免费赠送服务次数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 99.9%，高于 99.5%	最长停服时间≤30 分钟	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%
低于 99.5%，高于 98%	最长停服时间≤120 分钟	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%
低于 98%	最长停服时间不小于 300 分钟	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%

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），以便于身份核验服务（API）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产品及服务。

(4) 用户采集信息主体身份信息时应获得信息主体同意并且符合相关法律法规要求。因用户未合法获得信息主体授权，造成身份核实服务连带责任损失的，用户应向数字认证公司赔偿。

(5) 用户应按期足额缴纳相关服务费用。

(6) 用户应当在其业务系统中明确告知信息主体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。

(7) 数字认证公司拥有身份核验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；

(8) 用户应在约定范围中使用合同中的产品及服务。

(9) 用户对身份核验结果存疑时，应当采取其它手段进一步核对，并对自身业务行为独立承担责任。

(10) 用户保证向本公司提交身份核验申请前，已获得信息主体合法、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信息主体投诉或追究的，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（云服务提供商、可信数据源提供方等）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）数字认证公司不对身份核验结果的准确性、完整性作任何承诺，结果仅供用户内部决策参考，任何时候均不具备证明效力。

（4）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。

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。