附件1

采购项目需求

人脸识别系统H5实时活体检测产品

一、项目概况

（一）项目介绍

随着移动支付、数字身份验证和远程服务的普及，需要确保用户的真实身份以提高安全性和防止欺诈行为。传统的静态生物特征识别方法，如指纹、面部识别等，容易受到照片或视频攻击。因此，实时活体检测成为保障用户真实身份的重要需求。

线上化业务的发展，使得越来越多金融功能可以通过线上服务（APP、公众号、小程序等）提供给客户，为客户带来了便捷。

APP开发本身由于投入研发人力高，上线周期较长，且在推广过程中也需投入较多宣发费用，成本较高。因此H5实名认证方案正在逐渐成为各行业实名认证的首选方案。

（二）实施内容

本项目为按阶段完成H5实时活体检测落地实施，包括需求分析、开发、测试、上线实施、运行维护等，建设内容包括如下：

前端H5页面服务：用户与系统进行交互的界面，集成于业务APP中或通过H5直接进行服务调用，前端H5页面采集实时视频流、截图抽帧及压缩加密处理后，传送至后端服务。

活体检测模块：用于判断用户提供的人脸是否为真实的、活动的人脸，以防止使用照片或视频欺骗系统。该模块可以通过分析面部表情、眼球运动、头部姿态等特征，区分真实的活体人脸和静态的非真实样本，对各种呈现式攻击、注入攻击及新型黑产攻击可有效进行识别并拦截。

管理平台建设：搭建基于H5活体的应用管理平台，实现对活体检测规则及策略的灵活配置和记录管理。

（三）功能需求★

H5实时活体需纳入我社现有人脸识别系统进行统一管理，可在同一界面上实现系统管理、租户管理、账户权限、角色管理、SSO单点登录、API集中接入和管理等系统功能；同时需与我社现有人脸识别1:1系统进行无缝对接，在不改变现有业务流程和技术接口的情况下，完成活体检测和人脸比对。

1. 前端交互

H5实时活体通过获取手机视频流并进行压缩编码，经过加密后上传到服务端，活体服务端进行实时分析并给出实时反馈，支持动作活体、静默活体及炫彩活体，并可应用于微信公众号、H5页面端等场景。H5实时活体可对活检过程做实时检测，提示客户的不合规行为，帮助客户调整姿势和场景，提示内容包括光线、遮挡、多人、无人、人脸更换、距离等，可有效帮助客户根据提示纠正动作，快速通过活体验证。系统需采用数据加密技术保证传输过程中的数据的安全，在保证使用效果和流畅度的前提下，最大程度提高安全性。浏览器可支持移动端及桌面端主流浏览器型号及版本。

1. 前端交活体攻击防护算法

可防范如纸张图像攻击、面具攻击、视频回放攻击、抠洞面具攻击、裁剪面具攻击、高仿真3D面具攻击、头模攻击、电子屏幕翻拍、换人攻击、AI合成图像攻击、深伪合成图攻击、对抗样本攻击、真人视频注入攻击等多种攻击手段。

1. 后台管理

场景配置：支持对使用场景进行场景化配置，每个场景支持建立独立的动作规则，支持配置使用的引擎，以及回调地址，满足多渠道、多场景使用的个性化配置。

引擎管理：可查看当前系统中的引擎信息。

识别记录：记录使用过程中的检测记录，可查看检测过程中的影像资料，以及统计检测过程中的活体动作、引擎关键数据。

调用统计：系统后台支持对识别数据进行采集，并对数据提供全方位分析。分析包含引擎及渠道调用统计分析、引擎通过率分析攻击分布等。

降级管理：可通过平台配置不同的检测方案，可场景配置，自助选择该场景使用的检测方式，实现H5实时活体到视频活体的降级

系统管理：包括系统属性配置、数据字典及定时任务管理。

1. 非功能需求★
2. IT架构要求

应用系统须支持招标方同城机房应用双活部署、在线运行和同时使用，不受授权码（License）、用户数量及部署主机CPU数量等因素的限制。应用系统使用的第三方商用成品中间件（如TongWeb、宝兰德等）除外。

1. 应用架构要求

应用系统须满足招标方多级法人（省联社、审计中心、法人社/行）体系下业务管理和使用的同时，能支持招标方在其管辖范围内发起设立机构（如：村镇银行）的使用并满足应用和数据安全隔离性要求。

1. 硬件部署要求

应用系统支持主流国产操作系统、数据库、中间件等平台软件。应用系统须支持国产化 PC Server及国产化虚拟化等常用服务器硬件环境的安装部署。

1. 性能要求

1.系统整体性能支持我社未来8-10年的业务发展要求。

2.并发用户数是指同一时刻系统处理的请求数，系统应支持实时联机业务并发用户数不小于30 TPS。

3.系统资源占用率：为了保证系统能够正常、稳定运行，推荐配置的服务器在业务最高峰或批处理运行期间CPU占用率和内存使用率不应超过70%。

4.配合我社制定性能测试计划和验收标准，以及测试方案、环境、工具和调优策略（相应的报告文档），配合完成压力测试，确保系统能满足上述性能容量要求。

1. 系统灵活性及扩展性要求

要求系统支持主流国产化架构的硬件设备。要求系统具备松藕合特性，提供系统间标准交互接口。要求系统具备良好的可扩展性，支持面向贵州农信实际情况的二次开发及功能扩展。

1. 系统稳定性要求

系统服务进程在上述“4）性能要求”的条件下能不间断运行，系统须支持7\*24小时运行。

1. 安全性要求

采用有效技术手段，确保系统运行稳定，且系统信息符合我行信息安全基线要求。系统必须在整体架构、网络结构、应用系统、数据库等方面采取安全措施，提供相应安全措施方案，以确保符合安全性要求。

备份与恢复支持两级或三级存储架构设计，确保数据不会因为任意单点损坏而丢失。

建立系统应用及数据的定期备份机制，支持冷备和热备两种措施，对过期的备份文件设置定期清理机制，提供备份策略。

建立异常恢复机制，支持应用的热备，有效防范单点故障，保障系统运行的可靠性。系统须支持基于备份文件实现系统应用及数据库的快速恢复。

1. 数据要求

系统所产生的数据须符合行方制定的数据标准，如未达到，须按照数据标准对数据结构进行调整。

1. 服务地点

服务地点：我社指定的办公地点。

1. 实施要求

项目工期要求：服务商项目人员进场6个月。

服务商应根据项目工期要求，开展系统开发/实施/改造工作，按期完成本项目所有工作。如因我社单方面原因导致服务商工期受影响，服务商工期相应顺延。

为确保本项目的顺利实施，我社与服务商双方成立项目组负责项目开发实施过程中的工程进度、变更管理及双方的协调等工作；服务商应提供具有足够能力和经验的工程师参与实施。本项目开发实施过程中，服务商对项目人员（含项目经理）的任何调动和调整，须事先征得我社的（书面）认可。

二、服务要求★

（一）服务质量要求

项目服务全程符合我社的各种规章制度及项目质量要求。软件技术开发符合我社质量体系要求，提供给我社的应用系统源代码和技术文档符合我社的规范要求，且应用系统具有良好的可维护性。

（二）日常管理要求

1.服务商外包人员办公设备配备、网络接入、文档资料保存等应符合我社的管理要求，同时应保管好我社提供的物品、设备及项目资料，如有损失应照价赔偿。

2.服务商外包人员需要访问或使用的信息资产，按“必须知道”和“最小授权”原则进行访问授权。

3.考勤管理

（1）服务商保证技术服务人员在工作期间应遵守我社规章制度，根据我社外包管理人要求进行每日签到及签退，不得迟到、早退和旷工。

（2）外包人员工作期间不多于2天（含）的请假，在不影响工作进度安排的情况下，必须提前24小时向我社外包管理人请假。人力外包人员在工作期间的各种休假（多于2天的），在不影响工作进度安排的情况下，须提前至少1周向我社外包管理人提出请假并完成工作交接。

4.出差管理

（1）因项目和市场需要，我社有权要求服务商服务人员出差公干，服务商应按照我社要求派服务人员出差。服务商出差人员需按照要求完成出差任务并提交详细出差报告。

（2）我社安排服务商服务人员的出差和外派，发生的相关费用，包括交通、住宿、差旅补贴等，由服务商承担。

6.工作规范要求

服务商在开展工作期间，须严格遵守以下工作规范要求：

（1）遵守国家法律和政府的有关条例、规定和办法，以及我社相关管理规定开展工作；

（2）执行有关项目建设的法律、法规、规范、标准和制度，履行规定的义务和职责；

（3）服务商安排人员入场时，服务商人员须同步签订保密承诺书并严格履行承诺书条款。不泄漏各方认为需要保密的事项。

7.交付物管理

服务商应根据我社要求，将所有项目成果物交付给我社。

服务商应严格管理交付物版本，保证我社对于交付物各版本的可追溯性。

交付的所有文档均应提交电子版及印刷版，另有说明的除外，交付物内容必须与实际工作情况相一致，其质量必须符合我社的要求。

交付物为满足服务工作目标和相应技术、业务要求的文档，包括但不局限于：实施方案、系统源码、阶段性工作报告、工作总结报告、技术服务和技术服务相关资料。

（三）保密要求

1.除明确标识为公开材料的外，涉及本项目及相关的一切资料，均为保密材料，服务商应严格保密。

2.服务商服务人员首次进入我社工作场地工作时须签订服务承诺书，不泄漏所本项目各方认为需要保密的事项。

（四）知识产权

1.本项目中服务产生的所有成果的知识产权归我社所有。

2.服务商应向我社提供软件产品源代码。同时，在服务工作结束前，服务商应向我社提供服务产生的所有技术成果、过程文档、软件定制化部分产生的源代码、相关数据等，除软件定制化部分产生的源代码知识产权为双方共同拥有外，其余的项目成果归我社所有。

3.服务商保证其提供的服务及产品（包括服务中使用或添加于我社设备、系统上的硬件、软件、工具、模型、方法论、源代码、文档、知识资产）没有任何权利瑕疵，没有侵犯任何第三方权利。我社在使用该产品或服务的任何一部分时，免受第三方提出的任何侵犯其知识产权的权利主张。如果任何人对我社使用该产品及服务主张权利，由服务商负责处理一切纠纷及相关事宜，由此给我社造成的损失，由服务商承担。

4.如果第三方声称服务商向我社提供的产品或服务侵犯其知识产权，并就此对我社或服务商提起（包括威胁提起或很可能提起）法律诉讼程序或知识产权行政执法程序（以下统称侵权诉讼），我社有权：

（1）暂停履行对侵权诉讼所涉产品或服务的采购或支付义务直至侵权诉讼完全解决，并要求服务商自担费用向我社提供与该第三方协商、诉讼、和解所需的一切协助（包括但不限于向我社提供证明侵权不存在的各类证据、派出人员参加协商、诉讼或会谈等）。

（2）我社有权选择与该第三方达成和解，并由服务商支付和解协议所约定的全部费用以及我社因侵权诉讼而遭受的全部损失或费用（包括但不限于诉讼/仲裁费、律师费、交通费、通讯费、差旅费、对第三方的损害赔偿金、行政处罚罚款、获取该产品或服务相应使用许可的费用、因停止使用或修改、替换侵权威胁所涉及的产品或服务而遭受的损失等）。如我社选择继续参加侵权诉讼法律程序，服务商应当先行支付我社因侵权诉讼（包括仲裁或诉讼费、律师费、交通费、通讯费、差旅费等）及履行生效法律裁判而需支付的费用及损失，但生效法律裁判认定服务商产品或服务不存在侵犯第三方知识产权情形的，该部分费用由服务商向恶意诉讼的第三方追偿。

（五）服务违约及赔偿要求

1.服务商未经我社批准向第三方转包或转让本项目的一部分或全部的，我社有权解除本合同，服务商除退还我社已支付全部款项及银行同期贷款利息外，还应向我社支付项目合同总价款20%的违约金。

2.因服务商原因造成本项目开发工作失败的，服务商应退还我社已支付的全部合同款项及银行同期贷款利息，并按合同总金额的20% 向我社支付违约金。

3.服务商保证所开发的项目产品不存在任何缺陷和质量问题，不存在任何技术上的漏洞。我社在安装、使用服务商开发的技术成果过程中，发现因服务商原因导致的缺陷或瑕疵的，我社有权要求服务商在接到我社通知并在我社书面通知规定的时间内免费进行修复；如因该缺陷或瑕疵给我社造成损失的，服务商应赔偿我社全部损失。若超过我社规定的时间仍然无法修复或无法达到正常使用的，我社有权终止合同，并要求服务商退还全部款项及银行同期贷款利息，并按合同总金额的20%向我社支付违约金。

4.如服务商向我社提交的技术资料、图表、说明等不符合要求的，服务商应在发现或收到我社通知后 3 日内免费予以更正、补齐或更换。逾期未更正、补齐或更换的，服务商自逾期之日起按本项目合同总价款的1‰乘以逾期天数向我社支付违约金；因此给我社造成损失的，服务商应赔偿我社全部损失。

5.因服务商技术人员不遵守安全操作规程或不遵守我社规章制度等给我社造成损失的，服务商应当赔偿我社全部损失，并且我社有权解除合同。如有以下行为的，每人每次服务商向我社支付 2000 元的违约金：

（1）服务商人员私自联入我行网络系统；

（2）服务商人员工作计算机同时接入内网和外网；

（3）其他违反规定的行为。

6.服务商违反本我社相关保密条款的，除支付项目合同总金额 20 ％的违约金外，还应承担因此给我社造成损害的赔偿责任。

7.服务商未在故障响应时间内做出回应，或者未能在我社要求的合理时间内妥善解决故障的，服务商应当向我社支付人民币2000元违约金，该违约金不足以弥补我社损失的，服务商应赔偿实际损失，违约金和实际损失由我社从应付款中直接扣除，如果应付款不足扣付，服务商应当另行足额支付。