上海银行安全加固服务项目供应商征集公告及项目采购信息公示

（招标编号：SPM-ZBWJ-202304046）

项目所在地区：上海市

一、招标条件

本上海银行安全加固服务项目已由项目审批/核准/备案机关批准，项目资金来源为其他资金/，招标人为上海银行股份有限公司。本项目已具备招标条件，现招标方式为其它方式。

二、项目概况和招标范围

规模：每年一次安全加固服务，每次服务内容为：APP（含IOS和andriod）、小程序、H5、提供外部SDK等载体的安全加固服务，具体包括防反编译、防动态调试、防二次打包、数据和密钥加密等，不限上述载体数量，不限上述载体加固次数；同时，每次APP加固时，提供APP的自动化安全检测服务；为应对新浪每年测评服务，需要提供一年至少两次针对APP本身的人工安全评估服务，含APP侧个人信息及APP本身的安全评估

范围：本招标项目划分为1个标段，本次招标为其中的：

(001)上海银行安全加固服务项目;

三、投标人资格要求

(001上海银行安全加固服务项目)的投标人资格能力要求：（一）具有中华人民共和国境内依法设立且具有完全民事行为能力的法人。

（二）2020年1月1日至今，未因诚信问题、违法等行为被相关部门予以处罚、通报、或受到法律制裁。

（三）本项目不接受联合体参与，且入围后不得转包、分包。

（四）本项目不接受单位负责人为同一人或者存在直接控股、管理关系的不同供应商同时参加同一招标项目的投标。

（五）2020年1月1日至今供应商具有符合《网上银行系统信息安全通用规范》（JRT 0068-2020）要求的同类服务案例至少1例。

（六）供应商具有依法缴纳税收和社会保障资金的良好记录。

（七）供应商具有健全的财务会计制度。；

本项目*不允许*联合体投标。

四、招标文件的获取

获取时间：从2023年04月19日 09时00分到2023年04月24日 16时00分

获取方式：详见公告内容

五、投标文件的递交

递交截止时间：2023年05月26日 13时30分

递交方式：具体递交响应文件时间以发放的磋商文件为准纸质文件递交

六、开标时间及地点

开标时间：2023年05月26日 13时30分

开标地点：具体的磋商时间以发放的磋商文件为准

七、其他

上海市建设工程监理咨询有限公司受上海银行股份有限公司（以下简称采购人）委托，就“上海银行安全加固服务项目”进行供应商征集，诚邀合格的供应商参与，并对项目相关信息进行公示。

一、项目概况及内容

（一）每年一次安全加固服务，每次服务内容为：APP（含IOS和andriod）、小程序、H5、提供外部SDK等载体的安全加固服务，具体包括防反编译、防动态调试、防二次打包、数据和密钥加密等，不限上述载体数量，不限上述载体加固次数；同时，每次APP加固时，提供APP的自动化安全检测服务；为应对新浪每年测评服务，需要提供一年至少两次针对APP本身的人工安全评估服务，含APP侧个人信息及APP本身的安全评估。

（二）入围、价格有效期自入围通知书发出日起至2026年4月30日。

二、采购方式

竞争性磋商。

三、合格供应商资质要求

（一）具有中华人民共和国境内依法设立且具有完全民事行为能力的法人。

（二）2020年1月1日至今，未因诚信问题、违法等行为被相关部门予以处罚、

通报、或受到法律制裁。

（三）本项目不接受联合体参与，且入围后不得转包、分包。

（四）本项目不接受单位负责人为同一人或者存在直接控股、管理关系的不同供应商同时参加同一招标项目的投标。

（五）2020年1月1日至今供应商具有符合《网上银行系统信息安全通用规范》（JRT 0068-2020）要求的同类服务案例至少1例。

（六）供应商具有依法缴纳税收和社会保障资金的良好记录。

（七）供应商具有健全的财务会计制度。

四、服务要求（包含但不限于）

详见服务要求附件。

五、报名时需提交的资料

（一）工商行政管理部门或市场监督管理部门登记的企业法人营业执照、税务登记证、组织机构代码证或“三证合一”的《营业执照》或同等效力的文件（复印件并加盖公章）。

（二）法定代表人和被授权人相关资料。（1）法人身份证(复印件并加盖公章)；（2）被授权人授权书有效原件(加盖公章)；（3）被授权人身份证有效原件及复印件(复印件并加盖公章)；（4）被授权人姓名、手机、邮箱(复印件并加盖公章)。

（三）（1）2020年01月01日至今，投标人、法人及被授权人在中国裁判文书网（http：／／wenshu.court.gov.cn／）有关“贪污行贿”的查询截图并加盖公章，且无不良记录；（2）2020年01月01日至今，投标人、法人及被授权人在信用中国网站（https：／／www.creditchina.gov.cn／）有关“失信被执行人”、“重大税收违法失信主体”、“政府采购严重违法失信行为记录名单”的查询截图并加盖公章，且无不良记录；（3）2020年01月01日至今，投标人在国家企业信用信息公示系统网站（www. gsxt. gov. cn）有关“列入经营异常名录信息”、“列入严重违法失信名单（黑名单）信息”的查询截图并加盖公章，且无不良记录。

（四）本项目不接受联合体参与，且入围后不得转包、分包。（承诺书并加盖公章）

（五）2020年1月1日至今今供应商具有符合《网上银行系统信息安全通用规范》（JRT 0068-2020）要求的同类服务案例至少1例，并提供含签章页面的合同或客户证明材料等（复印件加盖公章）。

（六）(1)公告发布起12个月以内、连续三个月及以上国家税务机关出具的纳税或完税证明（复印件并加盖公章）；(2)公告发布起12个月以内、连续三个月及以上国家社会保障机构出具的社会保险参保证明（复印件并加盖公章）。

（七）提交近3年（2019、2020、2021）经审计的财务报表（复印件并加盖公章）。

注：以上资料原件或复印件加盖公章的扫描件发送至代理公司邮箱，资料如有缺漏，代理机构将拒绝接受。代理机构仅对供应商提供的资料进行审查，符合要求的合格供应商将有机会参与本项目的采购。

六、报名时间、地点

（一）报名时间

2023年4月19日-2023年4月24日，上午09:00至下午16:00时（北京时间，节假日除外）。

（二）报名方式

发送报名资料至以下邮箱：spmzjzx@126.com

七、有关单位或个人如对本项目采购信息有异议的，可以自本公示发出之日起五个工作日内，以书面或邮件形式向采购代理机构或上海银行提出。

八、联系方式

采购人：上海银行股份有限公司

联系地址：上海市浦东新区银城中路168号

联系人：汪老师

联系邮箱：wangzhr@bosc.cn

监督邮箱：caigouzhongxin@bosc.cn

采购代理机构：上海市建设工程监理咨询有限公司

联系地 址：上海市静安区汶水路261号41号楼

联系人：王伊莲　何老师

联系电话：021-64171887

联系邮箱：spmzjzx@126.com

上海银行总行采购中心

二〇二三年四月十八日

八、监督部门

本招标项目的监督部门为/。

九、联系方式

招 标 人：上海银行股份有限公司

地　　址：上海市浦东新区银城中路168号

联 系 人：汪老师

电　　话：/

电子邮件：wangzhr@bosc.cn

招标代理机构：上海市建设工程监理咨询有限公司

地　　址：上海市汶水路261号41号楼

联 系 人：王伊莲

电　　话：021-64171887

电子邮件：spmzjzx@126.com

招标人或其招标代理机构主要负责人（项目负责人）：_____（签名）

招标人或其招标代理机构：_____（盖章）

1、加固系统要求

1）具体加固技术要求见《1-1：加固技术要求清单》

2）启动延迟：加固后客户端启动时间增加量不超过原包的30%

3）加固包大小：加固包大小不超过原包的10%

4）CPU及内存使用率：加固后客户端运行时CPU及内存使用率增加量不超过原包的5%

5）加固系统除常规操作页面提供加固功能外，还需提供加固接口，支持招标方其他系统调用实现自动加固和检测。

2、升级服务

招标方享受中标商原厂升级服务，在服务期内，针对加固系统升级包，中标方能够在T+3天内完成加固系统的免费升级服务。

3、技术支持服务

1）中标商需提供原厂商的技术服务，并向招标方提供7×24值守的原厂热线联系电话。对于招标方的服务请求，中标商必须在30分钟内做出回应，对于远程不能解决的问题，中标商必须确保在2小时之内到招标方工作地点予以解决。

2）中标商需提供招标方在代码加固软件个性化、加固接口调用开发时的技术支持服务。

3）中标商需最少安排2名固定的技术支持工程师（在移动安全领域工作3年以上），对我行服务提供全方位支持。

4）APP自动化检测服务需覆盖Android、iOS、SDK的漏洞扫描能力，能够通过深度静态代码检测，动态攻击验证双重驱动，提供源代码保护、数据存储、通信传输、安全防范等检测能力。

5）中标商在服务期内需提供移动市场监控服务，针对钓鱼应用和盗版应用的快速察觉及快速下架。

4、培训服务

供应商提供每年最少2次的移动安全技术、安全开发方面的培训。

5、加固技术要求（加注“★”条款为基础条款，供应商应对本说明书基础条款明确响应）

1）Android应用加固

要求项	子项	具体要求参数
Android应用防代码逆向要求	★DEX加壳保护	支持对DEX文件进行整体加壳保护
	★DEX字符串加密	支持对DEX内的明文字符串进行加密保护
	★DEX类动态保	支持对DEX内的代码进行动态抽取加密，并

	护技术	且在类被执行时不解密类内全部代码，只对被执行到的方法函数进行解密
	★DEX虚拟化保护技术	支持DEX虚拟化技术（VMP），能够将DEX代码转换为自定义的虚拟机指令，并以自定义虚拟机进行解释运行
	DEX全量虚拟化保护技术	支持DEX全量虚拟化技术（ALL-VMP），能够将DEX代码的通过DEX虚拟化技术进行全量保护
	★SO加壳保护	支持对SO进行加壳保护，防止反编译
	防查看伪代码	支持对SO代码进行加密混淆，防止IDA的查看伪代码功能（IDA F5功能）
	★导入/导出函数隐藏	支持对SO内的函数表信息进行加密
	SO动态清除	支持SO动态清除技术，能够在SO执行过程中动态清除内存中的函数符号
	★SO防盗用绑定	支持将SO文件同应用进行绑定，防止SO文件被非法盗用
Android应用防二次打包要求	★完整性保护	支持APK完整性验证，防止被非法篡改、二次打包
	★资源文件加密	支持对应用内的资源文件、配置文件进行完整性保护，防止被篡改
	★签名验证	支持对APP的开发者签名进行验证，防止被篡改签名、非法发布
Android应用防数据泄露要求	★数据加密	支持对本次存储的数据库文件、JS文件、证书文件、配置文件等进行透明加密保护，防止查看和修改
Android应用防调试要求	★防动态调试	支持防动态调试，防止利用调试技术或工具对应用进行内存动态调试
	★防内存注入	支持防内存注入，防止利用内存注入技术对

		应用进行恶意代码注入
	★防内存dump	支持防内存dump，防止通过内存dump的方式分析内存数据
	★防xposed hook攻击	支持防止利用Xposed工具进行Hook攻击
	★防Frida hook攻击	支持防止利用Frida工具进行Hook攻击
Android应用环境风险检测与防护要求要求	防截屏	支持防止在应用运行过程中通过截屏非法窃取、捕获敏感数据，保护用户隐私数据安全、交易安全
	★防日志泄露	支持防止攻击者通过分析应用日志信息获取敏感信息
	★防设备root	支持设备Root检测，对应用运行环境进行检测，判断设备是否已经Root进，确认后能够阻止应用运行
	★防模拟器	支持防止模拟器运行，对应用运行环境进行检测，判断是否运行在模拟器上，确认后能够阻止应用运行
	防USB调试攻击	支持防止通过USB连接电脑对手机应用进行调试
	防网络代理	支持防止应用在开启网络代理的设备上运行

2）ios应用加固

要求项	子项	具体要求参数
iOS应用加固支持语言要求	★Object-C/Object-C++	支持对Object-C/Object-C++代码的iOS加固
	Swift	支持对Swift代码的iOS加固
	★C/C++	持对C/C++代码的iOS加固
iOS防代码	★控制流平坦化	支持在不改变语义的前提下，通过控制流平

逆向要求		坦化将控制流进行混淆处理
	★不透明谓词	支持对跳转逻辑的判断值进行隐藏，增加攻击者逆向分析的难度
	★符号混淆	支持对代码内的类名、方法名、函数名进行加密混淆
	★字符串加密	支持对字符串进行加密
	★虚假控制流	支持增加新的虚假控制分支，加大破解和分析原始控制流的难度
	★多样性混淆	支持随机化混淆，每次混淆代码不一样
iOS应用防调试要求	★静态防调试	在源代码内添加防调试校验代码，在函数执行时触发该保护功能，防止继续调试
	★静态防Inline Hook	在源代码内添加防Inline Hook校验代码，在函数执行时触发该保护功能，防止Inline Hook攻击
	★静态防Swizzling Hook	在源代码内添加防Swizzling Hook校验代码，在函数执行时触发该保护功能，防止Swizzling Hook攻击
	★静态防Frida hook攻击	在源代码内添加防Frida hook校验代码，在函数执行时触发该保护功能，防止Frida hook攻击
	★静态防Cycript注入	在源代码内添加防Cycript校验代码，在函数执行时触发该保护功能，防止Cycript攻击
	★静态防Reveal注入	在源代码内添加防Reveal校验代码，在函数执行时触发该保护功能，防止Reveal攻击
	★静态代码完整性保护	在源代码内添加防代码篡改校验代码，在函数执行时触发该保护功能，防止代码完整性被破坏

	★实时防调试	在APP运行时开启自动守护功能，随时对调试行为进行监测和阻断
	★实时防hook	在APP运行时开启自动守护功能，随时对hook行为进行监测和阻断 支持防Inline Hook 支持防Swizzling Hook 支持防fishhook
	★实时完整性保护	在APP运行时开启自动守护功能，对代码段进行完整性
iOS应用防二次打包要求	★绑定App包名	支持绑定app包名，篡改App包名将会导致应用运行闪退
	★绑定App签名	支持绑定app签名，篡改App签名将会导致应用运行闪退
iOS应用环境风险检测与防护要求要求	★防设备越狱	支持自动检测设备是否越狱，在已越狱的设备上自动阻止App运行
	★防日志泄露	支持对代码内的系统日志输出进行阻断，防止敏感信息泄漏
	APP模糊化保护	支持App后台切换过程的屏幕模糊化，防止信息泄漏
	★防网络代理	支持自动检测是否存在网络代理设置，当发现APP在启用网络代理的环境上运行时，APP会闪退处理，防止基于代理的抓包分析。
	防共享屏幕	支持自动检测是否存在软件共享屏幕行为，在共享屏幕时运行APP会闪退处理，防止基于屏幕共享软件的远程信息窃取、诈骗攻击。
	★防模拟器	支持自动检测是否在苹果电脑模拟器上运行，当APP运行在模拟器上时会闪退处理，防止基于模拟器的各种越权攻击。

	证书文件加密	支持对证书文件加密，防止对证书文件的非法读取
	证书文件绑定	支持对证书文件的绑定，自动绑定应用包名和签名，防止被非法盗用
iOS应用加固后审计与定位要求	★加固结果可视化	支持加固后输出的是混淆加密的源代码，能够直观查看加固后的代码。
	★代码逐行定位问题	支持代码逐行调试代码，准确、快速定位问题

3）H5应用加固

要求项	子项	具体要求参数
H5防逆向要求	★代码紧凑	支持自动删除*.html、*.js文件文件内的代码注释，降低敏感注释信息被恶意利用风险。
	★防格式化	支持阻止JavaScript代码格式化工具还原易阅读格式。
	★加壳保护	支持对JavaScript文件进行整体加壳保护，防止整体代码结构暴露。
	★伪造控制流	支持在JS代码内添加无效、无意义的虚假代码、死代码，包括虚假的控制流代码等，增加代码分析复杂度，并让攻击者分析和调试进入无意义的陷阱内。
	★字符串加密	支持对源代码的明文字符串进行加密保护，防止攻击者使用它来快速定位程序核心代码的位置。
	★常量混淆	支持对JS代码内的常量数字进行混淆加密，防止攻击者使用它来分析代码逻辑。
	★函数混淆	支持对JS代码内的函数名称、变量名称进行混淆加密，防止攻击者阅读分析、调试定位

		，增加破解难度。
	★控制流平坦化	支持对JS代码内的控制流代码进行扁平化混淆（如循环和条件转移语句等），使JavaScript代码可读性差，攻击者无法理解。
	★表达式混淆	支持将JS代码内的二元表达式转换成等价函数调用形式，增大破解者分析难度，有效隐藏、保护核心算法的原始逻辑。
	虚拟化保护(VMP)	支持将JS代码转换为自定义的JS指令代码，并且只有通过自定义的解释器才能执行，让攻击者无从破解，保护核心代码安全。
	★多样性混淆	支持使用随机化混淆技术，确保每次混淆后得到的代码（函数名、变量名）都不相同，提高攻击者分析的难度。
H5防调试要求	★防调试保护	支持对JavaScript源代码进行防调试保护，防止攻击者调试分析。
	★防控制台输出	支持屏蔽浏览器控制台的打印函数信息输出功能，从而隐藏输出内容，增加攻击者分析难度。
H5防盗用要求	★域名绑定	支持将JS文件同域名绑定，防止JS代码运行在非授权的网络域名。要支持绑定多个域名。
	应用绑定	支持将JS文件同应用绑定，防止JS代码运行在非授权的应用上。要支持绑定多个应用。
体积优化	★HTML文件压缩	支持对html文件进行代码压缩，缩减代码体积，提高下载、执行效率
	★图片压缩	支持对png、jpeg等类型图片进行压缩，缩减代码体积，提高下载、执行效率

4）SDK加固

要求项	子项	具体要求参数
防逆向	★Jar文件加壳保护	对Jar文件整体加密、加壳保护，防止反编译
	★字符串加密	对Java代码内的的明文字符串进行加密保护
	★虚拟化保护	将Java字节码转换为自定义的虚拟机操作码，以自定义虚拟机进行解释运行。
	★SO文件加壳保护	对SO文件进行加密加壳保护，防止反编译
	SO文件完整性保护	实现SO文件文件完整性保护校验，如果SO文件被篡改，则无法运行SDK，应用崩溃。
防调试	★防动态调试	防止利用调试技术或工具对应用进行内存动态调试
	★防外挂、修改器	防止各类游戏外挂、应用修改器、变速器
	★防Xposed hook攻击	防止利用Xposed工具进行Hook攻击
	★防Frida hook攻击	防Frida工具进行Hook攻击
防盗用	★SO防盗用绑定	支持将指定的SO文件同SDK进行绑定，防止SO文件被盗用
	绑定APK	支持将SDK同需要集成的APK的包名和签名进行绑定，防止SDK被盗用在其他APK上。
支持格式	★ZIP格式	支持加固*.zip格式SDK
	★AAR格式	支持加固*.aar格式SDK
	★Jar格式	支持加固*.jar格式SDK

5）小程序加固

要求项	子项	具体要求参数
防逆向要求	★代码紧凑	支持自动删除*.html、*.js文件文件内的代

		码注释，降低敏感注释信息被恶意利用风险。
	★伪造控制流	支持在JS代码内添加无效、无意义的虚假代码、死代码，包括虚假的控制流代码等，增加代码分析复杂度，并让攻击者分析和调试进入无意义的陷阱内。
	★字符串加密	支持对源代码的明文字符串进行加密保护，防止攻击者使用它来快速定位程序核心代码的位置。
	★常量混淆	支持对JS代码内的常量数字进行混淆加密，防止攻击者使用它来分析代码逻辑。
	★函数混淆	支持对JS代码内的函数名称、变量名称进行混淆加密，防止攻击者阅读分析、调试定位，增加破解难度。
	★控制流平坦化	支持对JS代码内的控制流代码进行扁平化混淆（如循环和条件转移语句等），使JavaScript代码可读性差，攻击者无法理解。
	★表达式混淆	支持将JS代码内的二元表达式转换成等价函数调用形式，增大破解者分析难度，有效隐藏、保护核心算法的原始逻辑。
	虚拟化保护(VMP)	支持将JS代码转换为自定义的JS指令代码，并且只有通过自定义的解释器才能执行，让攻击者无从破解，保护核心代码安全。
	★多样性混淆	支持使用随机化混淆技术，确保每次混淆后得到的代码（函数名、变量名）都不相同，提高攻击者分析的难度。
防调试要求	★防调试保护	支持对JavaScript源代码进行防调试保护，防止攻击者调试分析。
	★防控制台输	支持屏蔽浏览器控制台的打印函数信息输出

	出	功能，从而隐藏输出内容，增加攻击者分析难度。
体积优化	★图片压缩	支持对png、jpeg等类型图片进行压缩，缩减代码体积，提高下载、执行效率
支持平台	★微信小程序	支持对微信平台的小程序进行加固保护
	百度小程序	支持对百度平台的小程序进行加固保护
	★支付宝小程序	支持对支付宝平台的小程序进行加固保护
	华为快应用	支持对华为平台的快应用进行加固保护
	抖音小程序	支持对支付宝平台的小程序进行加固保护