**安信农业保险股份有限公司**

**堡垒机招标公告**

**一、招标人：**安信农业保险股份有限公司

**二、招标内容：**堡垒机

**三、报名资格要求：**

1. 集成商为具有在中华人民共和国境内注册的独立法人的生产厂商或其直接委托的代理人，注册资金不低于500万元，在金融业服务5年以上，提供营业执照复印件加公章。
2. 集成商需在上海地区有正式的分支机构。
3. 具备生产厂商认证的技术人员 2名以上。
4. 集成商必须有厂家针对此次采购的授权。

**四、售后服务要求：**

1. 集成商应为安信保险股份有限公司（以下称为甲方）提供及时周到的系统技术支持。
2. 集成商应确保为甲方提供7\*24小时技术支持服务，响应时间不应该超过1 小时，现场响应支持不应超过4小时。
3. 集成商所提供设备保质期均为三年（具有特殊要求的除外），集成商所提供的设备在保质期内因硬件、软件本身质量问题所造成的损坏或无法正常运行，由此产生的维修、更换硬件和软件故障排除等所需一切费用（包括工程师差旅费用等支出）由集成商负责。
4. 集成商应提供相应的备件支持，以便及时更换损坏硬件。
5. 集成商应在质保期后设备生命周期内有义务继续对系统设备提供维保服务，甲方将支付相应费用。
6. 针对以上要求，集成商可提供具体可行的有吸引力的合作方案。
   1. **验收：**
7. 所有设备均需提供安装服务，所采购设备（包括软件）安装都必须由生产厂商授权集成商执行。
8. 安装前由甲方信息技术部协同甲方行政办公室对货物的品牌、数量、包装等方面进行实物验收。集成商提供的所有包装的货物均应完好无损。如遇交付前已拆封的货物，甲方有权拒绝或要求更换。集成商交货时，必需提供所有产品原厂或总代理出具的供货相关证明。
9. 集成商根据甲方技术要求在甲方信息技术部指导下进行设备安装、调试，并由甲方信息技术部进行使用性能方面的验收。
   1. **报名方式**

有意参加投标者请于8月31日前将标书及相关材料递送至以下地址：上海市共和新路3651号农保大厦313室 马春霞收

商务联系人：马春霞

联系方式：021-66988267 macx@aaic.com.cn

技术联系人：卫金凯

联系方式：021-66988391 weijk@aaic.com.cn

**招标参数**

### 资质要求

|  |  |
| --- | --- |
| **项目** | **基本要求** |
| 厂商资  质要求 | ★拥有ISO9001质量管理体系认证**（提供加盖原厂公章证明）** |
| ★拥有省级以上高新技术企业资质 |
| ★拥有软件企业认定证书 |
| 产品资  质要求 | ★投标产品必须具备计算机软件著作权登记证书**（提供加盖原厂公章证明）** |
| 所投产品要求成熟度不低于7年，以软件著作权登记证首次发表日期为准 |
| ★投标产品必须具备计算机信息系统安全专用产品销售许可证**（提供加盖原厂公章证明）** |
| ★投标产品必须具备中国国家信息安全产品认证ISCCC**（提供加盖原厂公章证明）** |
| ★投标产品必须具备涉密信息系统产品检测证书**（提供加盖原厂公章证明）** |
| ★投标产品必须具备军用信息安全产品认证（军B级）**（提供加盖原厂公章证明）** |
| 专利  要求 | ★提供实现热备、集群模式下的高可用数据同步方法的技术先进性证明**（提供加盖原厂公章证明）** |
| ★提供实现灵活配置的多因素认证的技术先进性证明**（提供加盖原厂公章证明）** |
| ★提供实现大并发下稳定应用的技术先进性证明**（提供加盖原厂公章证明）** |

### 性能要求

|  |  |
| --- | --- |
| **项目** | **基本要求** |
| 设备类型 | **1U机架式一体化设备，内置应用发布中心** |
| 可管理设备数 | ≥300个 |
| 网络接口 | ≥4个千兆自适应电口 |
| 硬盘容量 | 内置存储≥1TB |
| 电源要求 | 单电源 |
| 高可靠性  要求 | ★支持双机热备，支持系统配置以及审计日志实时同步**（提供加盖原厂公章的截图证明）** |
| 支持集群部署，系统策略支持统一下发，后期升级扩容方式支持单节点扩容，无需进行软硬件的二次升级即可完成。  ★支持第三方负载均衡，并支持集群自带的负载均衡模块。**（提供加盖原厂公章的截图证明）** |

### 功能要求

|  |  |  |
| --- | --- | --- |
| **项目** | **基本参数** | |
| 支持协  议类型 | **图形终端协议：**RDP、VNC、X11  **字符终端协议：**Telnet、SSH  **文件传输协议：**FTP、SFTP  **数据库类型：Oracle：**PLSQL、TOAD、SQLPLUS、SQLDEVELOPER；**Informix：**DBACCESS；**Mysql：**MYSQLFRONT、HIDESQL；**SQL Server：**SQLserver（2000-2012）；**Sybase：**SCVIEW4**；DB2：**DB2CMD、DB2QUEST  **WEB应用：**HTTP、HTTPS  **KVM类:**DSR、DSVIEW、RARITAN、RARITAN\_CC等  ★**其它应用：**AS400、REALVNC、PGADMIN、PCANYWHERE、RADMIN、DameWare、CiscoASDM、VMware vSphere Client | |
| ★单点登录 | 上述所有协议类型均可实现单点登录，图形化应用无需安装任何客户端和控件即可实现单点登录，即通过堡垒机实现图形化应用发布功能 | |
| 支持IE代填类型包括 JS、flash、HTML5等特殊登录页面。**(提供加盖原厂公章证明）** | |
| ★无缝应用发布功能 | 要求以上所有图形化应用在实际操作环境中均可以正常使用且可自由调整应用的窗口大小，做到无缝发布，拖拽窗口应自然流畅，无卡顿现象，像是在本地运行应用程序一样**(提供加盖原厂公章证明）** | |
| 系统自身安全性 | ★IP自动禁止功能 | 系统支持IP自动禁止功能，对连续登陆账号密码错误的来源IP自动屏蔽，可通过管理员解除屏蔽。**（提供加盖原厂公章的截图证明）** |
| 帐号自动禁止和锁定功能 | 支持账号自动锁定功能，用户1分钟内连续输入账号密码错误，自动锁定该账号 |
| 自身健康检测 | 支持对应用中心状态、审计状态和端口状态是否正常工作进行一键检查。 |
| **★**console口管理 | 保证在特殊情况下通过console口连接。保证紧急情况能够用过console管理员密码或网络IP地址。 |
| 运维管理 | 运维方式 | 支持C/S与B/S运维方式 |
| 工具属  性支持 | 支持字符类putty、SecureCRT等工具的各类属性：终端属性、字符编码、窗口大小随意调整等等；图形类mstsc工具的原有属性：自定义开启/关闭磁盘映射、剪切板等，支持窗口大小随意调整、声音传输等等 |
| 授权审核 | 可以指定系统用户查看该用户可管理的资产信息；可以指定资源名/资产IP/账号名查看资产属于哪些系统用户管理。授权关系导出（可以导出用户和设备授权关系进行查看，导出展现形式excel） |
| 授权审批 | 运维人员可以在系统Web界面填写授权审批流程单，填写内容至少应包括：设备资源、系统账号、协议类型、时间窗口；审批通过后，运维人员可立即取得相应访问权限 |
| ★向导模式 | 为管理员和运维人员提供操作向导模式，方便用户进行设备管理和使用**（提供加盖原厂公章的截图证明）** |
| ★中英文管理界面 | 支持中英文切换WEB管理**（提供加盖原厂公章的截图证明）** |
| ★自动化运维 | 可以制定计划任务，至字符类资产执行事先编辑好的脚本。  脚本超时执行时间为每个计划在单台机器上的超时时间。执行超过超时间后会断开连接 |
| 可以通过手动登录某台资产，登录后会触发机器自行执行预先设置好的脚本。  可关联相应堡垒机运维帐号及资产帐号。 |
| 用户帐  号管理 | 用户角色 | 系统角色需按法案要求进行划分，至少有系统管理员、密码管理员、配置管理员、审计管理员、普通用户等多种角色。 |
| 身份认证 | 系统提供身份认证，自然人（员工帐户）登录系统时支持静态口令、Radius认证、LDAP、AD域、数字证书认证、动态令牌认证、USBKEY认证、指纹认证和Google手机动态令牌认证。 |
| ★支持指纹认证：  至少支持三个厂商的指纹认证。 |
| 系统内置PKI证书认证功能，用户只需配置USB-KEY即可实现证书登陆认证，实现双因素认证（USB-KEY+PIN码）。 |
| ★系统内置动态令牌认证，用户不需要额外部署认证服务器，通过配置动态令牌实现双因素认证；同时可支持Google手机动态令牌认证**（提供加盖原厂公章的截图证明）** |
| 支持多因子认证自定义组合，可为不同用户组分配不同的认证策略，支持单因素，双因素和多因素的认证策略。**（提供加盖原厂公章的截图证明）** |
| 批量管理 | 支持以excel格式批量导入和导出用户帐号 |
| 用户帐号自动改密，可制定改密计划对用户帐号进行定期改密，并发送邮件通知用户。 |
| ★在线批量编辑，提供堡垒机用户的批量编辑功能，以方便用户管理员批量修改帐号属性及关联信息，包括会同权限、用户状态、有效时间。**(提供加盖原厂公章证明）** |
| ★支持从AD服务器批量导入用户帐号**（提供加盖原厂公章的截图证明）** |
| 设备及账号密码管理 | 批量管理 | 支持批量导入导出运维用户、目标设备、账号密码等，支持目标设备账号批量新增 |
| ★支持在线批量设备帐号修改；支持设备帐号属性添加和修改，包括帐号密码、应用参数、帐号状态、会同信息、改密脚本、特权帐号、应用端口、应用密码提示、帐号类型、帐号提示符、帐号同步。**(提供加盖原厂公章证明）** |
| ★SSH公钥登录 | 通过ssh-keygen产生公钥和私钥密码对，上传堡垒机，可实现免密码登录服务器 |
| ★密函打印 | 支持将目标设备资产的账号密码进行密函打印导出**（提供加盖原厂公章的截图证明）** |
| ★设备账号  自动改密 | 支持linux、unix、网络设备、windows2000/2003/2008的自动改密功能；无需通过插件、引擎或特殊端口对目标设备进行自动改密， |
| ★在系统完成密码修改之后，自动进行新密码登录测试，以便进一步校验密码修改结果 |
| 权限管理 | ★分权管理 | 支持系统管理员按部门进行分权管理，各部门系统管理员只能管理和授权本部门管辖内的设备资源；支持审计管理员分权管理，只能审计被授权的设备。（**提供加盖原厂公章的截图证明）** |
| 访问控  制功能 | 系统提供访问控制功能，支持对系统的用户登录进行可配置的策略设置，根据策略因子：用户或用户组、日期、每月、每周、时间、源地址、目标地址、目标端口、目标账号、动作(接受、拒绝)来定制访问策略对用户或用户组行为进行控制。 |
| ★**提供禁审功能，可对部分设定的控制策略的会话不审计录像，防止机密信息二次泄露** |
| 命令控  制功能 | 系统可以对字符操作的命令进行控制，通过制定命令黑白名单实现对命令的有效管理，可以对命令集合进行告警或者自动阻断，支持正则表达式匹配。 |
| ★SFTP和FTP目录锁定 | 默认规定用户登录后，只能在其目录下进行操作，不能随意跳转至其他目录进行操作，也可通过开关打开限制（提供加盖原厂公章的截图证明） |
| 会同功能 | 系统应具备会同功能。如运维人员需要访问目标设备，首先需要向管理员申请连接会话，得到管理员同意后，运维人员才能对目标设备进行运维操作。 |
| 会话会同支持会同生效时间，且支持以web弹窗的方式通知会同授权人。会同人收到会同请求时，刷新页面或登录时会在页面弹窗提示。 |
| 日志审计 | 命令记录 | 支持命令记录：字符终端命令记录、图形终端键盘操作记录、数据库运维SQL命令、图形标题栏识别（OCR） |
| 字符终端命令记录：用户可以从任意命令开始查看本命令输出结果或播放；命令分析功能将输入命令和输出结果的智能分离，可以只查看字符命令，也可以显示该命令的返回结果 |
| 图形终端键盘操作记录：支持图形终端键盘操作记录，完整记录键盘动作 |
| ★数据库运维SQL命令：系统应具备审计到详细的SQL语句，而非键盘符指令，并要求记录到SQL语句的执行时间**（提供加盖原厂公章的截图证明）** |
| ★图形标题栏识别（OCR）：系统应具备对图形运维中的标题名进行智能提取，并可以从任意一个标题名开始回放。可支持中英文操作系统的标题栏体系。**（提供加盖原厂公章的截图证明）** |
| 录像记录 | WEB在线回放完整会话；字符终端操作会话支持倍速播放；图形操作会话支持拖拉定位播放；支持暂停、停止、重新播放等播放控制操作。 |
| 审计录像采用数据流回放技术，空闲操作（无屏幕变化）日志无增长，节省了日志空间 |
| ★传输文  件备份 | 系统应具备审计到FTP/SFTP传输的原始文件，并可以在审计系统上进行备份并下载查看其具体内容。对大于一定大小的FTP/SFTP运维审计中的文件可进行异地转储，并可记录文件md5值，保障文件的完整性和有效性。支持人工开关自由选择是否备份原文件。**（提供加盖原厂公章证明）** |
| 日志搜索 | 提供搜索功能，可组合目标主机地址、登录地址、堡垒机用户、远程账号、时间、键盘输入的命令、标题栏等条件进行搜索，快速定位会话记录；搜索条件“用户命令”支持“或”和“与”逻辑关系。 |
| **★**字符运维命令返回值搜索和屏幕导出，支持搜索命令的返回值信息，并支持将屏幕信息导出为文本。 |
| 告警模块 | 图形操  作告警 | 支持RDP会话针对操作行为告警（针对标题栏进行告警），可进行告警内容设置。 |
| 数据库  操作告警 | 支持数据库应用针对操作命令进行告警，可进行告警内容设置（告警内容支持动作，表名等）。 |
| 数据管理 | 数据存  储管理 | 存储告警：日志存储超过设置的阀值进行邮件告警，支持定期删除计划，只保留设置时间段的日志。 |
| 数据备  份管理 | 支持通过FTP和SFTP进行系统配置备份和还原，支持FTP和SFTP和本地方式进行审计日志的备份，系统配置和审计日志均可可自定义备份计划。 |
| 离线播放 | 导出日志可以使用离线播放器进行日志查看和日志检索，包括命令、录像、标题栏内容等。 |
| 统计报表 | 报表任  务周期 | 系统应具备在对系统制定报表任务时，可以配置时间周期，支持以图(柱、饼等)，统计、明细数据的方式表现。 |